



UNIVERSIDAD ABIERTA INTERAMERICANA.

TRABAJO FINAL.

**“El auge de los delitos informáticos, la intimidad vulnerada y la
solución del proyecto de Código Penal”**

Tutor: Dr. Gabriel Gonzalez Da Silva.

Alumno: Aguyaro Valenzuela Macarena.

Título a obtener: Abogada.

Teléfono: (011) 2253 5765.

Correo electrónico: M.aguyarov@gmail.com

Fecha de presentación: 3 de Febrero de 2020.

Sede: Centro.

¿Queréis prevenir los delitos? Haced que las leyes sean claras, sencillas, y que toda la fuerza de la nación se encuentre condensada para defenderlas, sin que, por el contrario, ninguna parte de la misma se emplee en destruirlas. Haced que las leyes favorezcan menos a las clases sociales que a los hombres mismos.

Cesare Beccaria

AGRADECIMIENTOS:

El más amplio agradecimiento a mi familia, por acompañarme siempre, por brindarme amor incondicional y ser un soporte fundamental para mí.

A la Profesora Dra. Graciela C. Boni por acompañarme durante una parte muy importante de la carrera y brindarme su sabiduría.

A mi tutor, Dr. Gabriel G. Da Silva, por acompañarme durante este proceso con paciencia y entusiasmo.

ÁREA:

- Derecho penal.
- Derecho penal constitucional.

TÍTULO:

- “El auge de los delitos informáticos, la intimidad vulnerada y la solución del proyecto de Código Penal”.

TEMA:

- Los delitos informáticos en el Proyecto de Código Penal de 2019-

Breve resumen de la problemática.

Mi objetivo es exponer la importancia que reviste actualizar totalmente el derecho penal a esta moderna rama denominada derecho informático. Si bien se conocen los corolarios de la globalización y las nuevas tecnologías un aspecto no contemplado periódicamente son los problemas que abundan en Internet y como se conciben hechos determinados que en otros ordenamientos jurídicos ya son considerados un delito.

A nivel nacional el Derecho no consigue replicar a esta nueva necesidad. La informática parecería avanzar a pasos agigantados sin que el derecho pueda seguirle el rastro, pero con la Cooperación Internacional puede tratarse este problema que tiene surgimiento en el actual siglo.

Al presente el anteproyecto del Código Penal regula este tipo, aunque dejando situaciones nuevamente fuera de la normativa, sin que esto obedezca a una razón específica. Lo destacable es que en un Título a parte, intenta legislar estas conductas que son fuente de preocupación para la sociedad.

Por otro lado remarco que mi objetivo no es criticar los esfuerzos legislativos, los cuales son apreciables por nosotros, los miembros de la sociedad, pero analizando la problemática desde el lugar que hoy tengo, como estudiante de derecho y con miras a convertirme en abogada; debo enfocarme en sugerir una tipificación que no se vuelva rápidamente obsoleta y a su vez cubra situaciones previsibles; todo esto para evitar la comisión de estas conductas. El primer paso a una solución debe ser la legislación y la integración de todos los países a un Convenio actualizado.

Luego la asignación de recursos para crear más fiscalías especializadas a nivel Nacional, acorde con la densidad poblacional; asimismo instruir a la Justicia y a los ciudadanos sobre esta problemática y como detenerla; orientar a los ciudadanos acerca de la forma de realizar la denuncia e incorporar técnicos especializados para que aporten su opinión y actuar profesional.

Palabras clave:

Argentina, delitos informáticos, anteproyecto del CPN, derechos personalísimos vulnerados, Convenios internacionales

Objetivos:

1. Generales:

- Identificar las causas que generan la producción de estos hechos.
- Explicar en qué consisten los cuatro pilares fundamentales, con el objetivo de brindar una solución plausible y lógica.
- Argumentar la necesidad de regular estos tipos para dar respuesta a las víctimas de delitos informáticos y asegurar la protección de sus derechos.

2. Particulares:

- Delimitar las conductas disvaliosas. Con el objetivo de contemplar la mayor parte de situaciones previsibles y así conformar la normativa planteada.
- Brindar una potencial solución con una ley y otras medidas que corresponden ser acogidas.
- Aspirar a una normativa que contenga palabras más amplias referidas a la tecnología para que la legislación no se vuelva obsoleta en un futuro cercano, de esta forma la norma se seguirá aplicando para los casos en los que corresponda siendo capaz de ser utilizada aunque haya una forma nueva de cometer estos delitos o algo de la mecánica para cometerlo se altere.

Hipótesis:

En la legislación penal vigente, los delitos informáticos tienen una regulación parcial y poco abarcativa de los tipos, o conductas tildadas doctrinariamente como disvaliosas, con el agravante de establecer sanciones laxas. Lo anteriormente expuesto incide en el crecimiento de estos delitos, de manera tal que solo se puede reducir este índice con lo que denomino: “los cuatro pilares fundamentales en el derecho informático”, los cuales consisten en: una normativa penal específica, la utilización de herramientas tecnológicas como instrumento de prevención; la cooperación internacional y políticas activas por parte del Estado.

Justificación en la elección del tema:

Mi interés sobre este contenido existe desde que descubrí la existencia de estas “conductas disvaliosas informáticas”; si bien este hallazgo fue paulatino; ya que analice distintos medios de comunicación, con el paso del tiempo, noté y me interesé por esta problemática que en Argentina no era solucionada de forma total pero en otros países tales como Estados Unidos; Brasil; España; sí lo eran.

A modo de confesión el disparador inicial, el que me brindó la inquietud sobre el tema que estoy tratando viene de la mano del Dr. Miguel Sumer Elías, él mismo brindó diversas entrevistas donde discute la privacidad en el internet, entre distintos aspectos vinculados.

La primera noticia que leí sobre esto fue en medios nacionales; luego en mi portal de noticias preferido; la “BBC”; a raíz de leer múltiples notas periodísticas y realizar una comparación sobre cómo era “tratado” el tema en diversos países es que observe nuestra legislación penal realizando especial foco en esta problemática.

En consecuencia descubrí que la ley N° 26.388 que modificó el Código Penal en el año 2008 no era capaz de comprender totalmente la problemática que surgía. En dicha ley se intenta legislar parte de algunos de los *hoy considerados* “delitos informáticos” pero agregándolos a tipos tales como violación de secretos, daños, etc; sin formar un tipo penal y obviando ciertos “hechos” del tratamiento legislativo. Esto que saco a la luz es relevante ya que se intentó dar una solución rápida sin comprender la magnitud de la problemática y así se dejó fuera de la legislación situaciones previsibles años más tarde. Por otro lado hay que reconocer un avance en materia de Grooming, mediante la Ley N° 26.904 la cual que regula, a su manera dicha problemática.

Para dar un rápido concepto al grooming es la conducta del que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma, conforme a lo establecido por el Artículo 131 del Código Penal.

Por otro lado el actual Artículo 128 introduce la figura de la pornografía infantil, esto también es considerado por la doctrina como un delito informático¹ ya que se considera que para ser posible se utilizan tecnologías de transmisión de datos.

Cabe contemplar que parte de la doctrina criticó el artículo en cuestión por no considerar dentro del tipo penal la “tenencia de pornografía infantil”. *Delpech* analiza esta cuestión y sostiene que *“el origen de esta no penalización, y que fue objeto de debates en el Congreso, fue no violar el art. 19 de la Constitución Nacional”* (Fernández Delpech, 2016, p. 208). No obstante en el año 2018 por medio de la Ley N° 27.436 esto se modifica y se incorpora la “simple tenencia” siempre y cuando el sujeto sepa que tiene en su poder el material; lo cual será pasible de diversos argumentos y excusas que presentaran imputados por este delito ya que debe probarse que el sujeto conocía la existencia de ese material.

Conforme seguí estudiando baraje otras opciones como tema de trabajo final, pero decidí defender esta idea porque me motivo profundamente la falta de amparo que tendrían y tienen las eventuales víctimas.

Es por todo esto que sostengo la necesidad de una reforma del Código Penal contemplando estos nuevos delitos y la actualización del Convenio de Budapest elaborado en el año 2001 y recientemente aprobado en el 2017 por medio de la ley 27.411. Por otro lado el mejor ejemplo de “cumplimiento” del convenio se puede observar en el anteproyecto del Código Penal de 2019.

Si bien fue novedoso para mí tratar esta nueva rama del derecho como lo es el “Derecho Informático” esto no impidió adentrarme en esta moderna línea de pensamiento y análisis sobre los temas que integran la misma.

Sobre todas las cosas tuve la suerte de encontrar un tutor que pueda acompañar este interés y brindarme más orientación sobre el tema dado éste no pertenece a una materia de la carrera; sino parte de especializaciones posteriores.

Problema jurídico relevante:

El problema aquí planteado son los delitos informáticos y su multiplicación rauda con el paso del tiempo. Las soluciones estudiadas comprenden: la sanción de normas penales, la Cooperación internacional; otra parte de la doctrina destaca que es imprescindible “acción por parte del estado” sin especificar si se refiere a legislación, control, o alguna otra medida de protección hacia los usuarios.

En el marco de la solución ubico a los “cuatro pilares fundamentales”; los mismos son una combinación entre todo lo expuesto por diversos autores, los cuales claramente están en lo correcto pero me vi obligada a plasmar un cuarto agregado. Estos agregados conforman “pilares fundamentales” como bien mencione anteriormente; de esta forma la combinación de distintas enmiendas propuestas por variados autores con el adicionado de: la utilización y actualización en materia tecnológica como instrumento de prevención de estas conductas informáticas; así como la especificación de las “acciones por parte del Estado” las cuales son traducidas como “Políticas activas por parte del Estado” brindan la solución al problema; siendo el mismo desarrollado y contestado. Pese a esto pueden derivarse otras situaciones que pueden motivar dudas a las que se intentará responder.

Es por esto que el problema jurídico relevante se relaciona con distintos ejes, en un primer lugar la inexistencia de una norma específica que regule **integralmente** los tipos, una norma distinta a la ley 26.388; que no omita pronunciarse sobre diversas situaciones; las cuales expondré a lo largo del trabajo final.

Además el planteo sobre esta temática, valiente pero insuficiente, del anteproyecto del Código Penal de la Nación, la desprotección que sufre y sufrirá toda víctima, hasta que la norma atienda el problema y por último las herramientas que debe otorgarle la legislación al juez para que imparta justicia.

Introducción.

Con el correr de los años las normas que conforman el derecho han ido variando en función de distintas problemáticas que fueron trascendiendo. Es por esto que se sostiene que el derecho es de carácter dinámico.

Así es notorio que mediante el paso de los años el derecho transformó distintos institutos y se ha ayornado para dar réplica a los requerimientos de la sociedad. A su vez esta sociedad que fue evolucionando en distintos aspectos ha logrado como parte de su desarrollo social “la tecnología”.

En este trabajo me dedicaré analizar una cuestión vinculada a internet y la web, específicamente a los delitos informáticos.

Este no es un tema poco menor, los delitos informáticos no tienen frontera y toda actividad cometida en internet se expande en segundos y teniendo en cuenta que pueden cometerse delitos utilizando como herramienta el internet, el derecho es el único que tiene la autoridad de poner un alto, de trazar los límites.

Al decir internet y web parece estar hablando de lo mismo pero no es así.

El internet es una red de computadoras que está conectada entre sí y no tiene una “frontera”, es decir una delimitación física, sino que su carácter es internacional. Internet nació en el año 1969 con el nombre Arpanet y rápidamente fue evolucionando a lo que se conoce actualmente. Ya en los años 90 se consolidó como una nueva tecnología.

Por otro lado la web también surgió en los años 90 de la mano de un informático llamado Tim Berners-Lee. La web está controlada por las páginas que conocemos, que tienen un dominio en internet y que están asentadas en esa red de computadoras conectadas entre sí. En conclusión utilizamos internet para acceder a la red.

Desde su comienzo hasta el siglo pasado era de público conocimiento la web 1.0; en la cual los usuarios solamente podrían ver contenido y leerlo sin tener la facultad de interactuar o establecer una comunicación sin límites como actualmente sucede.

Algo para destacar es que actualmente contamos con la web 2.0 la cual surgió en el siglo pasado y hace que se comparta la información de una forma más dinámica y facilita la interacción entre usuarios.

Y dentro de este camino de la globalización, de las nuevas tecnologías y de los avances, es que se está mencionando el inicio de la web 3.0 dónde se incorpora la Inteligencia artificial.

Volviendo sobre el eje principal, menciona Fernández Delpech que surgen posiciones diferenciadas respecto a lo que son los delitos informáticos. Una de estas corrientes es la autorregulación y dentro de ellas se encuentra la opinión de que el ciberespacio es libre y por eso debe autorregularse; entonces habría una absoluta libertad de los partícipes para determinar las reglas en cuanto a su comportamiento por internet (2016, p. 9).

Esto llama poderosamente la atención porque no puede haber total albedrío en algo que pasó de ser un escueto canal de comunicación a un estilo de vida, es decir la exposición que tienen todas las personas en internet.

Siguiendo con la postura del autor mencionado se contempla a los partidarios de la regulación, los cuales consideran que no existe diferencia en cuanto las actividades llevadas a cabo en la red con aquellas similares, llevadas a cabo en el mundo tridimensional y consecuentemente no existe razón para excluir la ley ordinaria a ciertas actividades cuya única particularidad es que son llevadas a cabo en forma electrónica (2016, pp. 9-10).

Él es partidario de esta última corriente ya que la primera corriente implica la negación del derecho, es decir, optar por no regular lo vinculado a estas conductas.

Y es que coincido con la postura del autor debido a que no hay que perder de vista las actividades de las personas en tanto conciban un daño. Y que si hay un daño y/o delito no se debe mirar con el rabillo del ojo debido a la vulneración de derechos que emerge.

Entonces el derecho y la ayuda de la informática a mi parecer son las únicas herramientas con las que contamos, que son competentes para disipar el asunto en cuestión.

La tecnología sirve como una herramienta para simplificar diversas cuestiones del día a día, pero desde hace unos años este instrumento tan valioso trajo consigo un grupo de problemas para los miembros de la sociedad y el derecho aún no ha dado una solución adecuada.

Es un error creer que la informática por más avanzada que este pueda superar el derecho, ya que el mismo es una creación del hombre, del legislador y el mismo lo va moldeando según los requerimientos actuales, por su estructura dinámica. Indudablemente creo que la informática podrá ser alcanzada y regulada.

Actualmente considero que el derecho debe salvaguardar a los individuos de ciertos hechos que se están cometiendo vía internet.

Estos delitos que en Argentina no están sancionados en su totalidad, en otros países del mundo lo están.

Son llamados delitos informáticos porque se cometen vía internet.

Algunos de los tipos que voy a explicar incluyen: introducir visual y/o auditivo y/o audiovisual; de carácter íntimo o privado a la red de internet y/o plataformas sociales sin consentimiento de la o las otras personas causando de esta forma un daño patrimonial o extrapatrimonial; la creación de una identidad falsa, apropiándose de la de un tercero con el fin de producir un daño patrimonial o extrapatrimonial; o creando una para sí o para otro con el fin de cometer hechos delictivos; el robo de datos en línea, la compra y venta de sustancias ilegales, armas o personas, la creación de sitios web ocultos o el ingreso a los mismos para cometer un acto delictivo; entre otros.

- Breve referencia al marco legal. -

Algunos de los delitos informáticos han sido tratados por la ley 26.388. Esta ley modifica parcialmente algunos de los artículos y ha introducido el término “informático”. De esta forma intenta legislar este nuevo tipo, a mi parecer de forma incompleta. Por otro lado la ley 26.904 la cual solo legisla un tipo denominado por la doctrina como: Grooming.

De aquí desprende una nueva idea que es la cooperación internacional.

Respecto a la cooperación internacional Argentina suscribió el Convenio de Budapest en el 2017 aunque el convenio tiene más antigüedad aún.

En materia de estos delitos internacionalmente debe haber una cooperación para detectarlos investigarlos a tiempo y reunir la prueba necesaria.

En el cuadro jurídico transnacional la seguridad informática pasó a ser una de las principales preocupaciones y de ahí en adelante se empezó a regular jurídicamente para sancionar esos hechos y disminuir el índice de esos delitos.

No es una cuestión menor el medio por el que se comete el delito ya que la persona que utiliza este medio muchas veces trata de ser no identificado empleando una serie de maniobras para disfrazar su dirección IP.

Comprender esta problemática trae aparejado la necesidad de explicar algunos términos.

Cada computadora conectada a una red tiene una dirección única, una especie de “huella digital” y se denomina dirección IP.

Para cometer un delito por este medio *en algunos casos* se oculta o modifica la dirección IP, es decir la dirección es manipulada con el fin de no ser descubierto. Una IP puede crearse o suplantar otra existente y también puede redirigirse hacia otro país.

Los usuarios de internet ingresamos a los buscadores más conocidos con el fin de acceder a distintas páginas web.

Lo que se está acrecentando actualmente es la utilización de buscadores paralelos que no tienen una dirección indexada a los buscadores conocidos y llevan a páginas de internet donde hay una comunidad delictiva. Por esto me refiero a lo que se llama la web profunda o Dark web. Esto no es objeto de mi análisis ya que estos delitos cometidos por este medio son clasificados por la doctrina especializada como “cibercrimen”; por no tener una motivación personal sino solo de tipo económico y contar con una gran organización en el actuar. Lo que aquí será tratado son los delitos informáticos per se.

El razonamiento aquí planteado sostiene que: todo daño que se cometa por internet en la mayoría de las ocasiones esta premeditado, es decir, no suele ser una conducta poco pensada, generalmente hay una planificación y además de esto la persona que utiliza este medio para dañar a otra, teniendo otros medios posibles, es totalmente consciente del impacto que su acción tendrá en la víctima. Por esta y otras razones que se plasman en este trabajo es que se deben regular estas acciones disvaliosas; tal como lo propone el Proyecto de reforma del Código Penal de la Nación.

Asimismo el que utiliza internet para cometer un delito o una conducta disvaliosa sabe de buena tinta sobre la masividad del contenido, es decir, en el caso de un obrar para perjudicar a un tercero es claro que lo que se busca es que sea masivo para poder generar más daño y de esta forma se demuestra que el sujeto es consciente de cómo eso afecta a la víctima en su psiquis, vida profesional, económica y/o familiar.

Lo clave aquí es hacer mención de la motivación para cometer estos delitos; aquí no se presenta una necesidad insostenible para un sujeto, la cual lo obliga a actuar en contra de la ley, tampoco hay un trasfondo socioeconómico que sea condicionante en su actuar; en este caso lo que mueve al sujeto son intereses particulares, de dañar a otro; sea en su patrimonio y/o en la esfera extra-patrimonial. Contemplado esto se debe impartir un tratamiento distinto; ya que la única parte débil es la víctima; esto lo relaciono directamente con el artículo 41 del Código Penal, siendo que aplica como atenuante en su inciso 2°.

La edad, la educación, las costumbres y la conducta precedente del sujeto, la calidad de los motivos que lo determinaron a delinquir, especialmente la miseria o la dificultad de ganarse el sustento propio necesario y el de los suyos, la participación que haya tomado en el hecho, las reincidencias en que hubiera incurrido y los demás antecedentes y condiciones personales, así como los vínculos personales, la calidad de

las personas y las circunstancias de tiempo, lugar, modo y ocasión que demuestren su mayor o menor peligrosidad (...) . (Código Penal de la Republica Argentina, 1985)

Sin la intención de extenderme de más inserté el artículo en cuestión ya que, en primer lugar **planteo la falta de aplicación de atenuantes para estos delitos**; en principio no deberían aplicarse las condiciones del inciso 2° ya que no hay presente: *“una miseria o la dificultad de ganarse el sustento propio necesario y el de los suyos”*.

Ahora si bien es cierto que no hay normativa específica en el Código Penal sobre los delitos informáticos lesivos de la órbita *extrapatrimonial* de la víctima; el Código incorporó mediante la ley N° 26.388 el término “informática” y lo lazo a “documentos”, “datos” haciendo extensible el uso de la expresión; lo cual considero que no es correcto por todo lo expuesto anteriormente, además de hacer posible que diversas situaciones queden incomprendidas.

Corresponde que exista una figura propia para los delitos informáticos, indicados en un título a parte, por la autonomía de este tipo en exclusivo; tal como lo presenta el proyecto del Código Penal.

Y es manifiesto que este tipo de delitos puede afectar a cualquier persona con o sin acceso a internet. Esto último lejos de ser algo fuera de lo común puede plasmarse en el siguiente hipotético: Dañar en cualquiera de las formas posibles a una o más personas que puedan o no tener acceso a las plataformas sociales, ultrajando su buen nombre, honor, reputación, violando su intimidad y que la víctima y/o su entorno social visualice el contenido generador de daño.

Apunto también a no tener que subsumir conductas con otros delitos ya tipificados debido a que la pena es menor y no sería proporcional a los delitos cometidos utilizando internet, además del deber existente de respetar la proporcionalidad entre la pena y el hecho cometido.

Hace aproximadamente diez años era impensado realizar una denuncia por un tema de esta magnitud, lo cual no quita el daño que se haya ocasionado en un sujeto y es por esto que se debe dar una respuesta urgente e integral para evitar que estas conductas disvaliosas proliferen y pasen de ser simples conductas inmorales y repudiables, a un tipo penal.

Es de carácter notorio que una parte sustancial para identificar la comisión de un delito es la denuncia de la víctima, en los casos que corresponda por ser de instancia privada, en cambio en otros casos al ser de acción pública el Estado podría intervenir directamente cuando se presenta alguna de estas situaciones.

Esta clasificación de delitos de instancia pública o privada forma parte de uno de los ejes importantes a debatir sobre a cargo de quién debe estar la denuncia según qué tipo de delito informático sea.

Por otro lado se debe contemplar que existen tres fiscalías especializadas en delitos informáticos, en CABA, debemos tener en cuenta que necesitamos sumar otras, es decir más gente especializada en estos delitos.

En un marco internacional y de legislación comparada que examinaré en el capítulo correspondiente compararé la legislación de otros países y se podrá observar el adelanto de los mismos en el tema. Y es que en otros países quizá más desarrollados los delitos informáticos y en específico la seguridad informática es un tema hondamente relevante y está dentro de la agenda.

Como país al estar atrasados en algunas cuestiones es importante que nuestro derecho no siga la misma suerte, es tarea de los juristas impulsar el avance normativo requerido por la sociedad.

Y con modificar la legislación sobre delitos informáticos que tenemos actualmente no me refiero solamente a agregar un “par” de artículos e intentar con eso detener un problema que avanza a pasos agigantados. También me refiero a incorporar un eje de participación internacional para poder de forma conjunta solucionar un problema que no tiene fronteras. Por esto los cuatro pilares fundamentales atenderán al problema en cuestión.

El uso de internet es moneda corriente en el transitar de nuestros tiempos y es que la mayoría de las transacciones que realizamos las hacemos vía internet y no sólo las transacciones sino también compartir una parte de nuestra vida, como puede ser en nuestras redes sociales, exponernos sin saber quizá hasta qué grado. Inocentemente se cree que es hasta donde uno lo permita, pero los delincuentes pueden encontrar la forma de sacar provecho económico de cualquier situación que este a su alcance o meramente generar un daño. Y no solamente un delincuente informático puede vulnerar derechos patrimoniales sino también cualquier sujeto que haga uso de internet y tenga intenciones maliciosas, inclusive generando la situación de vulnerar moral y psicológicamente a un sujeto.

Por otro lado un tanto alejado de lo mencionado en párrafos anteriores, se debe analizar la situación de las fiscalías, ¿cómo hace una persona que no se encuentra en la capital para realizar una denuncia de forma personal? Si bien algunas provincias cuentan con una delegación de informática esto no es la regla y tampoco la mejor idea para dar pronta atención a los afectados. ¿Qué sucede con una persona que ha sufrido un

delito informático y necesita la especial atención de una persona que esté debidamente preparada para atenderlo? ¿Es posible atender exitosamente todos los casos si contamos solamente con tres fiscalías especializadas? Lo claro es que se debe, a lo largo del país y según la densidad poblacional aumentar estas fiscalías e incorporar expertos en delitos informáticos.

Pero se debe dar cuenta de que este es un problema que no requiere solamente una sanción sino también la prevención porque es fundamental para evitar la proliferación de conductas no deseadas.

Y por último a mencionar, dentro de este trabajo una parte importante del mismo es el análisis de los derechos vulnerados con estos delitos; en líneas generales adelantaré que los mismos están bajo el amparo de la Constitución Nacional. Para sintetizar el fondo de la cuestión dentro del Capítulo pertinente me expediré sobre esto y analizaré los derechos vulnerados; pero el denominador común es el derecho a la intimidad, es por esto que daré un breve adelanto del mismo, utilizando una fuente prestigiosa.

En las palabras del Vicedecano de la Universidad Abierta Interamericana (Comprender el derecho, Conferencias de la Universidad Abierta Interamericana, 2014) :

El derecho a la intimidad es una manifestación inmediata de la personalidad a partir de la cual surgen facultades al modo de un derecho subjetivo específico extrapatrimonial. Bueres señaló que las posibilidades de disposición de estos derechos personalísimos (como cuando disponemos de nuestra imagen) demuestra la existencia de ese bien jurídico que la persona puede disponer y exigir su protección.

El Profesor y Dr. antes mencionado manifiesta que es posible afectar la libertad de intimidad por cuestiones que hacen al orden público por ejemplo la seguridad; pero encuentran un límite en la espectacularización de la intimidad. De esta forma, el autor concluye con que usar a la persona como objeto de espectáculo es lo que repugna al sistema jurídico Argentino y al internacional. (Comprender el derecho, Conferencias de la Universidad Abierta Interamericana, 2014)

El derecho a la intimidad es uno de los más vulnerados en estas prácticas o “delitos” informáticos; entre otros derechos sobre los que me expediré en el capítulo pertinente de mi trabajo final. Siendo un derecho que es arrancado de la víctima por el accionar del victimario merece un especial análisis dentro de mi trabajo, con el fin de apreciar de lleno en esta órbita como se afecta a la víctima de estos “delitos”. Utilizar

comillas en la palabra delito va de la mano con la explicación que realizo aquí y en mi trabajo final, la cual demuestra que por el principio de legalidad en materia penal no es posible denominar delitos a conductas disvaliosas que aún no han sido sujetas a legislación emanada de autoridad competente.

Relacionado íntegramente con el derecho a la intimidad se encuentra la “libertad”; pero no en un plano estrictamente físico y esto se distingue a simple vista si se contemplan algunos de los delitos que mencionaré; ya que por ejemplo la difusión, sin consentimiento, de la imagen de una persona no afecta su libertad física; pero si otras esferas de esta.

Un jurista de nacionalidad Mexicana, Lic. Riande Juárez, sostiene que dentro de un marco liberal el concepto de derecho a la intimidad y a su vez a la vida privada, se presenta como un derecho a la libertad, en cuanto derecho que tiene el individuo a hacer lo que le parezca; y a modo de ejemplo sostiene:, a no ser incomodado, a tomar decisiones dentro de su ámbito privado sin que el Estado intervenga en las mismas; como puede ser la libertad sexual, de revelar o no las conductas íntimas y el derecho que goza sobre la libertad a su identidad (1998, pág. 1) .

Siguiendo esta línea de pensamiento la libertad y el derecho a la privacidad están ligados. Cuando se “filtra contenido” de carácter privado, sin la autorización de la o las personas que figuran en él, hay una clara violación a estos derechos y

Esto se ve potenciado por el uso del internet y la mayor exposición que tienen las víctimas. Por lo anteriormente expuesto queda plasmada la obligación de atacar la causa y por ende debemos invertir en tecnología y expertos para combatir este problema.

Será cuestión de tiempo, pese a que quizá faltan recursos para que este problema aumente notablemente.

Y pese a que hay otras cuestiones que requieren especial atención no debemos descuidar está sino crear un balance.

Capítulo 1- “El derecho penal y sus espacios olvidados.”

1. Apertura del capítulo 1°

La informática a lo largo de estos años se ha introducido de lleno en la vida de las personas, pasando a ser parte de la misma. Los cambios generados por la globalización se extendieron a todas las áreas de la vida cotidiana. La creación de nuevas tecnologías vino de la mano de las plataformas digitales como aplicaciones y redes sociales. Estas cambiaron la forma de realizar transacciones, viajar y hasta de relacionarnos. Las redes se convirtieron en una extensión de la persona; así es como todo esto impacta de lleno en la vida diaria. Los aspectos positivos de esta nueva dinámica del corriente siglo, son públicamente conocidos sin embargo los aspectos negativos que de aquí se desprenden son comparables con la punta de un iceberg.

De esta manera el derecho, encargado de regular todo tipo de relaciones, tuvo que adaptar su teoría no sólo para la protección de la información y los dispositivos sino para el mejoramiento de procesos jurídico-administrativos. Para este último caso se creó una nueva área, la informática jurídica, donde la tecnología es puesta al servicio del Derecho. La misma se divide en Informática Jurídica Documental, orientada a la compilación y búsqueda de documentos jurídicos; Informática Jurídica Administrativa o de Gestión, concebida como ayuda a los procesos jurídico-administrativos tradicionales; y la Informática Jurídica Decisional, que busca suplantar decisiones humanas mediante el uso de programas automatizados de software. En cuanto a la informática como objeto de estudio, es a través del Derecho Informático es donde se aplica las reglas jurídicas con los problemas vinculados con la tecnología. Dentro de este campo existe un área relacionada con el derecho penal, que consiste en el estudio de aquellos delitos donde la informática desempeña un papel condicionante, tanto como medio para la comisión de un ilícito. Así, estos tipos de ilícitos son entendidos como delitos informáticos, delitos de alta tecnología o delitos cibernéticos. (Sain, El derecho penal aplicado a los delitos informáticos. ¿Una política eficiente para el cibercrimen?, 2013, p. 1)

El presente capítulo ya se centra en la nueva realidad, los “delitos”¹ informáticos como una consecuencia que surge de las nuevas tecnologías.

1 Aclaración pertinente sobre la utilización del término: me expido en el punto “2” del presente capítulo.

Un nuevo desafío que se le presenta al fenómeno jurídico es abandonar el ámbito clásico y abrir paso a las nuevas tecnologías, para no omitir la protección de ciertos derechos subjetivos.

Cuando me refiero al “ámbito clásico” hago mención de las situaciones que existen en el mundo físico, es decir, un robo, la producción y venta de material explícito sexual de menores de edad, etc. Y no por nada me referí a esos tipos, en la actualidad esto mismo sucede en el ámbito de la web pero de una manera no tan similar. Así se observa, el robo de datos informáticos, la pornografía infantil, entre otros. Aquí lo determinante es el uso de internet como una herramienta perfeccionada para cometer conductas disvaliosas, apuntando a generar un daño y contemplando la característica explícita de la herramienta: “la masividad del contenido”. Es que todo contenido que se publique podrá ser “viral” es decir observado por personas de distintos países, una publicación puede dar la vuelta al mundo en menos de un día, esto es porque en internet no hay límites.

Daniel Altmark sostiene que hay una parte de la Doctrina donde él está posicionado y allí se acepta la existencia del derecho Informático y a su vez este es entendido como una rama autónoma perteneciente al derecho, luego infiere en que la consecuencia lógica es el reconocimiento de un "Derecho Penal Informático", que se ocupa de los "delitos informáticos" que, a su vez, tienen un bien jurídico protegido que le es propio (Altmark & Molina Quiroga, 2012)

En el año 2008 se modificó el Código Penal y se han incluido algunas figuras relacionadas con los tipos informáticos, pero siendo la última reforma penal la del año 2018 aún hay conductas disvaliosas referidas a los delitos informáticos que no se encuentran tipificadas.

Resalto que es esencial ayornar nuestras normas a los fenómenos de la actualidad debido a que no puede quedar un hecho sin sanción por no tener una legislación actualizada. Aquí el eje del presente trabajo “la desactualización normativa” por falta de previsión y acuerdo legislativo en pos del bien de la sociedad en su totalidad. Estos nuevos tipos son los que abarcaran este capítulo y se evidenciará la urgencia de su incorporación como una figura. Pero lejos de apuntar a un positivismo extremo donde crea que la única solución a una problemática es la creación de una ley propondré lo que a mi parecer facilitaría detener este tipo de conductas, pero claro, una ley debe contener la acción en cuestión

las herramientas necesarias para detener el fenómeno y uno de los ejes más importantes en materia de delitos informáticos, la cooperación internacional. En el centro de este trabajo está la protección de los derechos subjetivos, la urgencia de que el derecho responda otorgando las herramientas para actuar ante situaciones que lo merecen, el avance de las nuevas tecnologías. Al tratar temas de esta índole hay que tener presente que estas conductas disvaliosas pueden versar sobre “porno venganza” o la “creación de identidades falsas”, entre otras, las que suceden por medio de internet, donde la masividad del contenido es aún mayor que la que se podría haber dimensionado hace diez años. Sin embargo recién en el año 2018 un grupo de legisladores reparan en esta cuestión y no completamente con la ley 26.388 “ley de delitos informáticos”, lo cual es un antecedente pero sin dudas no fue suficiente el esfuerzo volcado en tal redacción normativa, ya que la situación actual pudo haberse previsto.

Dicho esto pueden nacer varios interrogantes, pero el que debemos responder es el importante, ya que no puedo apartarme de mi tema central, ¿Por qué derecho penal? ¿Por qué no derecho civil? Pues bien, el único derecho que podrá tildar o clasificar como atípicas estas conductas informáticas disvaliosas es el derecho penal.

Así se origina el deber de remitir al contenido del derecho penal, el que está dirigido a lograr que los hombres actúen del modo que se considera necesario o conveniente para una ordenada vida social, permitiendo al individuo el goce de los bienes que ella les puede proporcionar.

Es el derecho en general a través de sus distintas ramas el que determina cuáles son esos bienes prohibiendo las conductas que tienden a menoscabar, desequilibrar su base, con el derecho penal y teniendo esas conductas y discriminando las que entre ellas se consideran de mayor incidencia en el quebrantamiento del orden social, se debe su protección.

El derecho penal es el conjunto de leyes o normas que describen delitos mediante la asignación de una pena delimitando las circunstancias de su realización, tendiendo a intensificar en esos casos la protección de bienes jurídicos mediante la acentuación de su prevención, delimitando a la vez la potestad del estado de castigar con la pena al determinar cuáles son las conductas ilícitas punibles. (Creus, 2010, p. 1)

2. Principios en materia penal

Enrique Bacigalupo; como se citó en (Tarrío Suárez & Tarrío, 2015), “*sostiene que se puede definir al Derecho penal subjetivo como el conjunto de condiciones que determinan la legitimidad de la amenaza y aplicación de penas por parte del Estado*”. (2015, pp. 101-102)

Esto es relevante ya que desembocará de manera directa en las garantías dadas por la Constitución Nacional, que son fuente de los principios en el derecho penal.

Dicho esto, siguiendo con la postura del Dr Tarrío, por un lado “*las garantías representan las seguridades que se otorgan para impedir que el goce efectivo de los derechos sea conculcado por el ejercicio del poder estatal, ya en forma de limitación del poder o de remedio específico para repelerlo*” (Tarrío Suárez & Tarrío, 2015, p. 102).

Dentro de las garantías penales destacaré las que considero vinculantes mencionar para el buen desarrollo del presente trabajo. Así recurriendo a los conceptos del Dr. Zaffaroni, se considera que:

1) La *legalidad*, consiste en ser un acto emanado del Poder Legislativo, de alcance general y abstracto, el cual puede definir qué acción u omisión de una persona es punible como delito y cuál será la pena que le corresponderá al infractor. Además sólo podrá aplicarse pena a quien incurra en la conducta descrita por la ley como delito, nunca otras no atrapadas por aquella descripción (todo lo que no está penalmente incriminado, estará penalmente permitido), ni con una especie o cantidad diferente de pena que la prevista.

2) La *irretroactividad* de la ley, está relacionada con el principio de legalidad; la ley debe regir para futuro y debe ser previa a la comisión del hecho, que es el momento de la acción. Solo será retroactiva si es más beneficiosa para el reo.

Estas garantías se sintetizan en la conocida máxima *nulhim crimen aulla poena sine proevia lege poenali*, contenido en el artículo 18 de la Carta Magna. Como precisiones de lo expuesto, se admite en forma generalizada que sólo pueden conminarse como punibles comportamientos; no pensamientos, ni condiciones o situaciones personales: se pena por lo que se hace o se deja de hacer. (Zaffaroni, 2005, pp. 98-103)

De esta forma las garantías deben estar presentes desde el principio, cuando se inicia la persecución de la persona y en los momentos posteriores; no solamente en el momento de establecer la pena aplicable. La existencia de las garantías explicadas

anteriormente encuentra su origen en el articulado de la Constitución de la Nación. De esta forma se reconoce el derecho o principio de reserva, la irretroactividad de la ley, entre otras.

El artículo 18 establece que: ningún habitante de la Nación puede ser penado sin juicio previo fundado en ley anterior al hecho del proceso (principio de irretroactividad de la ley), ni juzgado por comisiones especiales, o sacado de los jueces designados por la ley antes del hecho de la causa (juez natural). Nadie puede ser obligado a declarar contra sí mismo; ni arrestado sino en virtud de orden escrita de autoridad competente. Es inviolable la defensa en juicio de la persona y de los derechos. El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación. Quedan abolidos para siempre la pena de muerte por causas políticas, toda especie de tormento y los azotes. Las cárceles de la Nación serán sanas y limpias, para seguridad y no para castigo de los reos detenidos en ellas, y toda medida que a pretexto de precaución conduzca a mortificarlos más allá de lo que aquélla exija, hará responsable al juez que la autorice.

De esta manera el artículo 19 esgrime que: las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe. (Principio de legalidad o reserva). (Constitución de la Nación, Ley N° 24.430)

Con el presente marco constitucional las garantías en materia penal se plasman en el Código de forma y la doctrina realiza la interpretación pertinente.

Esta explicación y enunciación se debe al contenido del trabajo final, como mencione ut supra. Fue inevitable traerlo a colación ya que cuando hago alusión a “Delitos informáticos” e incluyo en la misma definición conductas que están contenidas únicamente en el anteproyecto del Código Penal o en otras legislaciones interpreto una violación al principio de legalidad; esto se debe a que en la actualidad hay tipos que no están contenidos en el Código Penal de la Nación ergo no está fundado en una ley emanada de autoridad competente.

* Entonces atento a esto es que tomaré el “permiso” de en alguna ocasión utilizar este término en mi trabajo, debido a que es un concepto ya instalado que no requiere de abundante explicación para delimitar el contenido del tema a tratar. Para no

abusar de este “permiso” en otras ocasiones lo reemplazaré con el término “conductas disvaliosas”, ya que entiendo que si pueden denominarse de esta forma.

Lo que sucede al designarlas de esta manera es que será preciso aclarar constantemente a que conductas me refiero; en este caso será a las cometidas mediante internet con el fin de causar un daño en la esfera patrimonial y/o extra-patrimonial a uno o más sujetos.

De alguna forma en el Código Penal de la Nación se mencionan palabras como “elementos informáticos, sistema o dato informático, manipulación informática” para tratar de suplir la falencia legislativa sobre el tema. No obstante sigue sin establecer un nuevo tipo, independiente, autónomo, denominado “delito informático”, por esto es que utilizo un permiso para emplear el término sin que sea descalificado. En la vereda contraria se encuentra el Proyecto del nuevo Código Penal, el cual será tratado en el capítulo correspondiente, atento al índice.

Claro está que las garantías son esenciales para todo proceso judicial. Las mismas resguardaran los derechos subjetivos de las partes y aspirarán a que no se cometan irregularidades.

Por otro lado, debo mencionar que por el Artículo 75 inc. 22 la Carta Magna dota de jerarquía supra legal a algunas Convenciones o declaraciones; una de ellas es la declaración universal de los derechos humanos, la cual en su artículo 11 reza:

1. Toda persona acusada de delito tiene derecho a que se presuma su inocencia mientras no se pruebe su culpabilidad, conforme a la ley y en juicio público en el que se le hayan asegurado todas las garantías necesarias para su defensa.
2. Nadie será condenado por actos u omisiones que en el momento de cometerse no fueron delictivos según el Derecho nacional o internacional. Tampoco se impondrá pena más grave que la aplicable en el momento de la comisión del delito. (Declaración universal de los derechos humanos)

Esto tiene relación con lo anteriormente establecido, ya que gozan de especial protección internacional las situaciones nombradas y contenidas en nuestra legislación; por otro lado no podemos vulnerar ninguna norma y/o garantía en pos de “hacer justicia”. No obstante tampoco se debe dejar de lado que ciertas conductas al no tener una tipicidad establecida (por imprevisión del legislador sobre las nuevas prácticas tecnológicas) generan vulneraciones graves a los sujetos que la sufren.

Sobre esto hare hincapié en el pertinente capítulo, “La vulneración de derechos constitucionales en la red”.

Ofrecida esta explicación, supongo ineludible referirme a la Teoría del delito, ya que en otro apartado me expediré sobre “las novedosas conductas susceptibles de ser tipificadas” es por esto que debo introducir el tema de la manera correspondiente, analizando: ¿Cuándo hay un delito?

Indica Eugenio R. Zaffaroni en la estructura de la teoría del delito, que el mismo acontece una vez que reúne las siguientes características (parte de su teoría) que el sujeto realice una acción, que sea típica es decir, que obedezca a una norma del legislador; que sea antijurídica y culpable. Por otro lado considera qué se debe excluir del concepto de delito toda pretensión de ejercicio del poder punitivo sobre cosas, animales, personas jurídicas, como también el que quiere ejercerse sobre personas *por algo que no sea una acción* es decir por el color, género, nacionalidad, condición social, salud, y en relación a la voluntad de una persona como puede ser que: lo empujen, arrastren o arrojen. (2005, p. 292)

Así continua sosteniendo que esta es la consagración teórica del “*nullun crimen sine conducta*”, pero no cualquier acción humana puede ser relevante como base teórica para el concepto reductor del delito. (...) Todo pensamiento, sentimiento, disposición, imaginación que no trasciende al mundo exterior no puede servir de base teórica para el delito. Cuando el pensamiento se manifiesta en el mundo sin duda estamos ante la existencia de acciones. El autor da el ejemplo de una injuria la cual es la expresión de un pensamiento que causa un perjuicio alguien. “No puede tolerarse que el poder punitivo avance con pretexto de conflictos insignificantes o de acciones que no son conflictivas o que claramente pueden resolverse por otras vías” pero conflictos que presentan estas características hay muchos y las agencias políticas criminalizan primariamente sobre algunos mediante instrumentos legales; que fijan el supuesto de hecho o tipo penal que se apoya la selección criminalizante secundaria. Esto es elastizar los tipos penales. Apunta Zaffaroni que el análisis de la tipicidad no puede ser puramente descriptivo sino que debe ser también valorativo, como parte sustancial de la tarea valorativa incumbe al teórico precisar en cada caso, si no se trata de un embutido arbitrario, de una realidad en el entendimiento del tipo; de una novedad inaudita. (Zaffaroni, 2005, pp. 288-289)

Es por esto que el autor también considera qué no puede constituir un tipo una acción que puede resolverse por otra vía y si pensamos en esta clase conductas

informáticas disvaliosas, se pone de manifiesto que lo único pasible de ser reclamado en sede civil serían los daños y perjuicios derivados de algunas conductas; pero para la “porno venganza”, el “hacking” “la suplantación de identidad mediante internet”, entre otras se vulneran varios derechos reconocidos en la Constitución, en la declaración Americana de los derechos y deberes del hombre, en la Declaración Universal de los Derechos humanos y en la Convención Americana de Derechos humanos; por mencionar algunos. Es claro que estas acciones no pueden contenerse y evitarse exclusivamente desde la normativa civil y de ahí el pedido de una justicia penal que se expida sobre el caso, que proteja los derechos consagrados en la Carta Magna y en todas las convenciones o instrumentos reconocidos en la Constitución por tener supremacía supra legal y de una justicia que también esté del lado de la víctima; porque aquí no hay duda, se requiere una tutela judicial efectiva. En esta línea de pensamiento ubico al Ante proyecto del Código Penal de la Nación, el cual considera en un título a parte dar tratamiento a los hechos mencionados en el presente trabajo final; pero el cual analizaré pertinentemente, ya que podría ser mejor en algunos aspectos; pero que sin lugar a dudas es un enorme avance en materia de derecho penal y que posiciona a la Argentina en un lugar cercano a otros países.

Observo que no operan permisiones por parte de la ley para que entre los particulares se presente la vulneración de derechos subjetivos, a excepción de la legítima defensa, claro; pero no hay una ley que autorice vulnerar la privacidad de una persona **excepto sea** para salvaguardar el bien público.

Dicho de otro modo lo que ocurre en las redes sociales cuando se provocan ciertos daños de tipo grave; los cuales afectan psicológicamente a la persona y a todos los aspectos de su vida; se debe actuar en pos del bien común y de no desproteger los intereses de todos los usuarios de redes sociales y/ o de internet.

Realizando un anticipo sobre los temas a tratar y comparando tipos penales sostengo que no puede ser equiparado con el delito de injuria un delito informático ya que versa sobre una publicación que afecta a la persona y es mediante una red social siendo además que este contenido versa sobre su vida íntima.

Se puede concluir añadiendo que todo aquel que no apoye esta vertiente claramente estará manifestando su propio pensamiento; lo cual está permitido Constitucionalmente y por vivir en una sociedad democrática; pero el fondo del mismo revela que el derecho a la intimidad, libertad e identidad no es de carácter trascendental.

3. ¿Nuevas formas de cometer delitos?

Según Sain, la expresión delitos informáticos refiere a aquellas conductas indebidas e ilegales donde interviene un dispositivo informático como medio para cometer un delito o como fin u objeto del mismo. En este sentido, los delitos informáticos son entendidos respecto al lugar que ocupa la tecnología para la comisión del delito más que a la naturaleza delictiva del acto mismo. (Sain, 2018, p. 10).

Señala Temperini que:

La informática posee como característica la transnacionalidad la cual demanda un desafío para el Derecho y en especial para los sistemas jurídicos penales, que deben concebir la necesidad de ciertos niveles mínimos de coordinación, que permitan un combate eficaz de este tipo de actividad delictiva. (Temperini, Delitos informaticos en Latinoamerica, un estudio de Derecho comparado, p. 1)

Una de las primeras definiciones fue la aportada por Donn B. Parker (1976) investigador y consultor en seguridad de la información; citado en (Hernandez Diaz, 2009, p. 231); él definió los abusos informáticos como *“cualquier incidente asociado con la tecnología de los ordenadores en el que la víctima sufrió o pudo haber sufrido un daño y el autor, intencionadamente, obtuvo o pudo haber obtenido un beneficio.”*

Desde un punto de vista criminológico, existen dos enfoques, en cuanto a la naturaleza de este nuevo tipo de fenómeno criminal; el primero de ellos es que los delitos informáticos no son más que delitos convencionales que toman nueva vida a partir del uso de dispositivos informáticos y de servicios y aplicaciones en internet. La segunda perspectiva afirma que las tecnologías de la información y comunicación brindan nuevas herramientas para la comisión de delitos inexistentes, como la distribución de virus o programas maliciosos a través de la red, ataques a sitios web y la piratería del software. Lo cierto es que ambos enfoques son ciertos.

Como sostuvo Sain:

Existen delitos tradicionales que adquieren nuevas formas a partir de la intermediación de dispositivos automatizados como también nuevas formas delictivas que no serían posibles de cometerse si no existiese un programa de software o archivos digitales presente, como, por ejemplo, en la elaboración de programas maliciosos con el fin de dañar un servidor web para afectar el funcionamiento de la página (...). (Sain, 2018)

Temperini afirmó que:

Entre todas las características que podrían desarrollarse sobre las tecnologías de la información y la comunicación (TIC), las principales son tres:

1. la inmediatez de las comunicaciones a distancia,
2. la posibilidad de la realización de acciones masivas,
3. la posibilidad de realizar acciones con un determinado nivel de anonimato. Estas tres características de las nuevas tecnologías son la materia prima necesaria para generar el efecto potenciador de los delitos. (Temperini, 2018, pp. 52-53)

La inmediatez de las comunidades a distancia esta entrelazada con la realización de actividades masivas. Se puede observar como en la actualidad todo contenido que es publicado en las redes puede llegar a cualquier punto del mundo, siendo “transnacional”, no teniendo fronteras; este quizá es el rasgo más desafiante para la órbita del derecho penal, pero no imposible, ya que la tecnología podrá ser utilizada también para prevenir situaciones como las que se desarrollarán en el presente capítulo.

3. 1 Las “novedosas” conductas susceptibles de ser tipificadas.

Como he planteado inclusive en el título de este capítulo hay nuevos accionares para perjudicar a terceros, los cuales sostengo son tipificables. Los mismos tendrán lugar producto del mal uso del internet. Con esto queda plasmado de forma expresa que el objetivo de este trabajo no es proponer restringir la libertad al navegar por Internet sino regular los casos donde por un mal uso de esta herramienta tecnológica se dañe a un tercero.

1- Suplantar la identidad de un tercero en una red social o cualquier plataforma digital. Introduciendo contenido verdadero o falso, es decir revelando secretos, o bien introduciendo datos falsos para generarle cualquier tipo de perjuicio.

El término “**spoofing**” utilizado por la doctrina y que se traduce como “suplantación” merece ciertas consideraciones que la doctrina comparte; así Matilde S. Martínez cita a Eduardo Molina Quiroga, quien contempla lo siguiente:

El robo, la usurpación o suplantación de identidad es un tema de vital importancia. A través de él los delincuentes utilizan datos personales para hacerse pasar por el sujeto al que le han robado su identidad. Estos robos, en combinación con el anonimato de las transacciones en línea y otras actividades; se utilizan para perpetrar una serie de delitos que comprenden desde el fraude hasta las actividades terroristas.

Señala Martinez que:

Dentro de esta modalidad se encuentra el fraude bancario, la extorsión en línea, el blanqueo de dinero y el contrabando con ayuda de computadoras y los delitos contra sistemas de computación y sus usuarios; con utilización de virus y otros programas hostiles, así como ataques de denegación de servicios. (Martinez, 2018, p. 44)

2- Difundir cualquier representación de la persona, sea visual o audio visual por medio de canales electrónicos, cualquier red social o plataforma digital. Siendo que el contenido pudo haberse generado a conciencia del perjudicado o sin que este supiera; pero sin que autorice dicha difusión.

Esto se refiere al “**revenge-porn**” más conocida como la porno-venganza implica “la publicación no autorizada de imágenes o videos privados, generalmente contenido íntimo, por parte de una persona (generalmente, la expareja por sí o a través terceros) que lo hace por venganza luego de terminar la relación. La Argentina no tiene tipificada la conducta. Los primeros casos de revenge-porn se intentaron resolver en la justicia penal por la vía de los delitos de injurias. Sin embargo, no se arribó a una solución judicial.

Una propuesta ante la situación fue presentada en el Anteproyecto de Código Penal del año 2014, presidido por el exjuez de la Corte Suprema de la Nación, Eugenio R. Zaffaroni. El artículo 120 del Anteproyecto establecía una pena de prisión de seis meses a dos años y una multa de diez a ciento cincuenta días, para el individuo que “vulnerare la privacidad de otro, mediante la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o imagen, o se apoderare de registros no destinados a la publicidad”. (Anteproyecto Código penal 2014)

Los fundamentos del Proyecto se dirigen a los casos de “pornografía de venganza” y los define como un problema de dimensiones globales. Además, las autoras del Proyecto sostienen que las NTIC y los dispositivos electrónicos para la producción de material audiovisual favorecen el uso de nuevas prácticas y conductas en los espacios de la intimidad sexual, de las que resultan imágenes o videos que son el resultado de un acuerdo entre las partes involucradas pero reducidas al espacio de confianza/privacidad en que fueron obtenidas. Hacen hincapié en los supuestos en que “por represalia, resentimiento, extorsión, venganza o sentimientos de animosidad respecto de sus exparejas o relaciones ocasionales de intimidad”, introducen en el

ciberespacio imágenes y/o videos que afectan la privacidad, la libertad y dignidad de las personas. (Anteproyecto Código penal 2014, 2014)

En Clarín (2014), (citado en M. Resio 2018) se publicó que: en los Estados Unidos, la Universidad de Michigan determinó que en el 90% de los casos de “pornovenganza” el agresor es un hombre y que cinco de cada diez víctimas admiten haber recibido fuertes insultos en las redes.

Más de 40 Estados americanos sancionaron leyes que penan el revengeporn. La vicepresidente de Cyber Civil Rights Initiative, la abogada Mary A. Franks, impulsó desde la organización sin fines de lucro el reclamo para combatir los abusos online. La profesora de Derecho Penal de la Universidad de Miami sostiene que existen 3.000 sitios web que publican pornografía de venganza, la cual es redistribuida a través de los medios digitales. (Resio, 2018, pp. 127-128)

Este caso quizá un tanto más delicado que otros, tiene aspectos en común con lo regulado para las personas menores de edad, sin discutir que el daño causado difiere ya que la edad de la persona en cuestión es un factor que tiene relevancia y tiene un impacto diferente en una persona menor y en otra mayor de edad. Insisto, la norma no puede discriminar en cuestión de edad, no se puede ser “permisivo” para quien realice dichas conductas y las dirija a una persona mayor de edad. Es absolutamente adecuado que la norma se expida en cuestión de protección infantil, es el deber que tiene, sancionar y tratar de prevenir en la medida que sea posible los casos; pero no puede descuidar otras situaciones.

Lo cierto es que estas conductas vienen en aumento y la norma es la única capaz de combinar elementos para prevenir y sancionar estas acciones.

Recientemente se han publicado investigaciones donde se revela que, “Facebook” ha desarrollado algoritmos capaces de detectar videos o fotos sensibles y que son difundidas masivamente en esa plataforma, con el fin de dañar a una persona. Llama poderosamente la atención que esta empresa de comunicaciones digital tome las armas necesarias para cambiar ciertas situaciones que ocurren allí. Cabe preguntarse dónde es que la ley actúa en estos casos, ¿Por qué aún no hay una ley que se expida sobre esto? ¿Los derechos inherentes a los sujetos que navegan en redes sociales no importan?

Merece especial atención y tratamiento este tema tan sensible para evitar la proliferación de estas acciones disvaliosas.

Planteo la siguiente hipótesis, si todas las páginas de internet tuvieran el mismo sistema para detectar estas conductas ¿la ley perdería su ratio legis? Considero que no, ya que podrían crearse nuevas formas de cometer dichas acciones disvaliosas y por otro lado se omite, generalmente, explicar cómo funciona este “mecanismo” empleado por Facebook. El mismo consiste en que la persona que sepa que será víctima de “revenge porn” contacte al soporte web de dicha aplicación y le envíe la foto. De esta forma es incorporada automáticamente y cuando sea publicada en Facebook por el victimario, la aplicación borrará dicha foto de forma inmediata.

En primer lugar debe destacarse que es una herramienta que no será muy útil, no toda persona tiene conocimiento de que será una eventual víctima, no toda persona tiene la foto o video que se filtrará y peor aún hay porcentajes de personas que son grabadas o fotografiadas sin su consentimiento, sea a solas o con un tercero, en el ámbito de su privacidad; por lo que será más difícil aun detectar estas situaciones.

Por otro lado creer que el único medio para difundir este “contenido multimedia” puede ser Facebook es un gravísimo error, ya que existen diversas páginas web donde se publica este tipo de contenido.

Como si el asunto no pudiera ser más grave aparecen nuevos casos de difusión de imágenes íntimas pero no están ligadas en su totalidad al “revenge-porn” sino a una combinación de maniobras y los “deepfakes”, así se utiliza una imagen de una persona y la introducen en una escena pornográfica sin su consentimiento, luego son publicados y las diferencias con un video real pasan desapercibidas.

i. Que la difusión sea para generar un perjuicio en su patrimonio, con fines de chantaje y/o para vulnerar su intimidad y exponerla públicamente. En este punto me refiero al denominado “**Sextorsion**” que consiste en: *“la extorsión a la víctima previamente filmada con el celular o mediante la cámara web del computador, solicitándole dinero para no difundir dichas imágenes o bien amenazándola para obligarla a ceder más imágenes de ella o de algún tercero”*. (Cherñavsky, 2018, p. 9)

Esta figura manejada por la doctrina y que se refiere a circunstancias por las que varias personas han transitado pueden tener como fin sacar un provecho económico, es decir disminuir su patrimonio a través de una extorsión, o bien tener el poder de la vida personal de esa persona, vulnerando su autonomía de la voluntad para publicar contenido no deseado de forma masiva y como represalia a cualquier hecho que lo anteceda, sin ser claro una justificación suficiente para generar el daño causado a la víctima.

Desde esta postura el derecho penal debe optar por regular esta figura y sus derivados (las que explicaré en este punto), o bien no dirigir la atención hacia un atentado contra la intimidad y la imagen de los sujetos que navegan en el Internet.

Atendiendo a las reflexiones que brinda la Dra. Nora Chernaavsky, la cual indica que según las estadísticas, muchas víctimas son las mujeres, considero relevante destacar la importancia de no impartir definiciones donde se excluya al género masculino, quien también puede ser susceptible de transitar una situación de estas características. Esto para nada apunta a la discusión de lenguaje inclusivo tal como se lo conoce actualmente, sino precisamente contemplar casos hipotéticos donde la víctima no solo puede ser la mujer sino también el hombre.

Si se quiere una norma y por tanto una justicia más justa no se deben hacer discriminaciones o distinciones por género, sino buscar el mejor espacio posible para que las personas que respeten la ley puedan vivir sin injerencias de terceros.

Es por esto que una definición más atinada se dedicaría a establecer que: consiste en que una persona extorsione a otra, exigiendo dinero o más contenido similar (llámese imágenes, audios y/o videos) para así no publicarlo/ difundirlo en redes sociales o cualquier plataforma de contenido digital.

Al apuntar “redes sociales o cualquier plataforma de contenido digital” es mi intención abrir el campo a nuevas formas posibles de interacción digital, para no acotar la lista a un *numerus clausus*, sino contemplar que tratándose de la tecnología es menester emplear términos que sean casi omnicomprendidos y así pueda preverse que estas acciones y contenido que dañe a terceros, se repita en un futuro y no encuadre legalmente por no ser una red social, o bien una plataforma digital. Con esto no apunto a la acción en sí, sino al medio por el que se logra, el internet; ya que en un futuro próximo con la inteligencia artificial quizá se generen situaciones nuevas y si la normativa es poco abarcativa quedará nuevamente fuera de la órbita del control jurídico.

Por otro lado la autora sostiene dicho postulado con base a datos de 2015 del Ministerio Público Fiscal de la Nación los cuales se refieren a consultas territoriales discriminadas por género donde el 70 % de dichas consultas corresponden a mujeres. Por eso mismo acompaño su pensamiento pero creo que al impartir una definición desde la corriente doctrinaria se debe ser un poco más abierto para no dejar cuestiones fuera de la órbita de tratamiento.

3- Crear, modificar para potenciar su peligrosidad, enseñar a utilizar, distribuir, publicar, un malware con el fin de vulnerar la seguridad de usuarios en internet y así causar un perjuicio patrimonial y/o extrapatrimonial.

Un ejemplo extremadamente atinado es brindado por el Dr. Marcelo E. Temperini, quien indica que en casos de cibercrimen podemos mencionar el ransomware, un software malintencionado, que tiene como objetivo “cifrar” el acceso a la información que contiene el equipo, para después poder pedir un “rescate” a cambio de su liberación. Estos casos son ejemplos donde los ciberdelincuentes no están interesados en la información particular de la víctima, sino en realizar de forma masiva, buscando un fin de lucro, que es el pago por el rescate. Es un negocio organizado, donde las bandas suelen estar compuestas por personas que se dedican a desarrollar el malware, otras a infectar sistemas. Otras quizás con menor organización, son las dedicadas a las estafas electrónicas (2018, p. 56)

4- Espiar comunicaciones, representaciones de una o más personas; en cuanto a su imagen y o voz, por medio de cualquier herramienta que pueda ser empleada vulnerando sistemas de seguridad o aprovecharse de su falta de seguridad, generando un perjuicio a la intimidad y el secreto de una o más personas;

Por el solo hecho de acceder a ese dato. En el caso de que se publiquen la pena debería mayor.

Esto puede ser conocido como **Spyware**, atento a la definición brindada por M. Martínez, se establece que es:

El que abarca programas que se instalan en el sistema o computadora, con la finalidad de rastrear nuestros datos y espiar movimientos por la red. Cumplida esa primera etapa se envía esa información a otro servidor para fines ilícitos. Se instalan cuando: se visitan sitios de Internet que descargan su código malicioso (también conocidos como: ActiveX, JavaScrips o Cookies) sin consentimiento del usuario; b) acompañado de algún virus; y suelen estar ocultos en un programa gratuito, los cuales al aceptar sus condiciones de uso permiten el espionaje. (Martinez, 2018, p. 43)

5- Crear representaciones de una o más personas para publicarlas sin su consentimiento con fines que no coincidan con el bien común o el orden público.

Esta es una nueva modalidad conocida como “**Deep fake**” donde se puede generar un video con audio de una o más personas a partir de una imagen. Esto es gracias a la inteligencia artificial. Pasar esto por alto, en cuanto a una regulación penal,

para prevenir su mal uso, implica responsabilidad por omisión. Es cuestión de tiempo hasta que la inteligencia artificial sea mal utilizada para generar perjuicios.

La desprotección en un internet sin fronteras implica la vulnerabilidad de los usuarios y por otro lado no dar herramientas con la ley para prevenir y sancionar este tipo de situaciones que pueden originarse, genera una situación de indefensión. Cuando la única herramienta que podría utilizarse para reparar, en parte la cuestión, no se utiliza, se vuelve inútil.

El **ciberstalking** es una nueva modalidad y según la doctrina que introduciré en las siguientes citas; puede ser definido como una conducta intencionada y maliciosa de persecución obsesiva; acecho o acoso respecto de una persona a la que se convierte en objetivo.

“Tiene que consistir en más de un acto manifiesto de persecución no querida por la víctima y que esta percibida como intimidatoria. Puede adoptar: cercar, vigilar, aproximarse, invadir las comunicaciones, allanar su vivienda (...)” (Alonso de Escamilla, 2019, pp. 217-218)

Un ejemplo claro para visualizar este punto atiende el siguiente hipotético: Un sujeto recibe constantes mensajes de una persona que puede o no conocer y manifiesta hacia el remitente su intención de que esto se detenga; bloquea a este sujeto y el otro busca la forma de seguir “en contacto”. También la situación puede extenderse al punto tal de recibir fotos recientes en un lugar (que puede ser público o privado), “sacadas” sin autorización de quien las recibe para transmitir un claro mensaje: ud. está siendo vigilado.

Las acciones aquí plasmadas encuadran en ciberstalking. Ahora bien, ¿Qué postura jurídica corresponde tomar para dar una respuesta proporcional? Por otro lado, ¿Importan la cantidad de mensajes, (audios o cualquier elemento que pueda enviarse), que la persona reciba? O ¿Basta con que manifieste que no desea recibirlos y ante esa advertencia el otro deba respetarlo?

Parte de la doctrina sostiene que *“la idea de persecución sin tregua ni descanso es la que le interesa al derecho penal”*. (Alonso de Escamilla, 2019, p. 218)

En algunos sistemas de derecho comparado se tipifican estas conductas como otro aspecto de la violencia doméstica pero al ser formas de acoso muy variadas que pueden tener lugar fuera de este ámbito tal opción deviene insuficiente.

Según Alonso D. E, vinculado a la violencia doméstica atiende el caso donde el acosador persigue a otra persona con la que ha mantenido una relación previa negándose a reconocer que ha terminado. Y esta es una motivación para que el acosador justifique su conducta y la víctima minimice su comportamiento. (2019, p. 219)

Observar estas conductas desde otros tipos de ópticas posibles es lo que hace mejorar las tipificaciones, no dejando escapar casos por no contemplarlos, por no poder descender los mismos a la realidad. Lo cierto es que las nuevas tecnologías traen consigo un conjunto de problemas y soluciones que hay que saber aprovechar.

Según Alonso de Escamilla, el *Stalking* tiene características especiales las cuales son determinadas por el medio en que se lleva a cabo:

- 1) El anonimato que proporciona la red y que sirve como pretexto para que el lenguaje del acoso cibernético sea más directo o violento del de la vida real.**
- 2) La situación de poder en la que se encuentra el acosador, gracias a ese anonimato del que goza en la red y; que puede utilizar tanto respecto de personas que ya conoce, como de las que conocen mediante internet.**
- 3) La información disponible por el acosador para entrometerse en la vida personal del acosado.**
- 4) El “mail bombing” para enviar contenido de forma masiva y “bombardear” al acosado.**
- 5) Colgar contenido ofensivo dedicado a la víctima por ejemplo amenazas.**

Estas circunstancias colocan al acosador en una posición de fuerza proporcional a la indefensión en la que se encuentra la víctima del ciberacoso.

El reto consiste en la elaboración de leyes que den respuesta a los supuestos mencionados, que se lleven a cabo mediante las nuevas tecnologías existentes y las que puedan surgir de forma previsible.

6- Publicar la comisión de delitos por redes sociales, plataformas de contenido digital, o internet; para incitar a que una o más personas comenten delitos.

Esta figura está ubicada en el ante último punto y se debe a que el bien jurídico susceptible de ser protegido, es notoriamente distinto a los contenidos anteriormente. Si bien me expediré sobre cuál es el bien jurídico protegido en cada caso, (y como estos derechos son vulnerados), en el Capítulo referido a “La vulneración de derechos

constitucionales en la red”. Sin embargo es preciso realizar la aclaración con el fin de comprender totalmente esta problemática; ya que no hay una ubicación al azar.

Siguiendo con esta corriente de pensamiento, no estoy proponiendo un “numerus clausus de tipificaciones”, mi intención es esbozar lineamientos generales para establecer nuevos tipos y que los mismos se ayornen conforme pasa el tiempo y la tecnología avance; pero al mismo tiempo reflexionar sobre los tipos penales en cuestión y hacerlos casi omnicomprensivos respecto a la evolución de las herramientas tecnológicas y no de las conductas cometidas ya que un tipo penal tampoco puede ser inexacto.

Estos casos a los que me refiero han sido conocidos durante estos años, donde se han publicado homicidios, actos de terrorismo, violencia física y/o psicológica; entre otros, en las redes o plataformas digitales.

Entonces, a lo que apunta este apartado es a sancionar a todo aquel que además de haber cometido un hecho claramente ilícito, utiliza internet para regocijarse de sus acciones, arengando a multitudes a seguir los mismos pasos o bien afectando a terceros que son involuntariamente espectadores de ese lamentable e injusto acto.

La doctrina no se ha expedido sobre este caso en particular y es por esto que no podré nombrarlo con un apoyo de fondo; lo cierto es que no por esto se debe pasar por alto esta situación. Con miras a ejemplificar reflexiono sobre un atentado terrorista que fue compartido en fragmentos mediante una transmisión en vivo por “Facebook”.

Estos actos realizados con la intención de animar a un tercero a cometerlos en conjunto o de forma individual son una clase de apología del delito, la cual se potencia por el medio tecnológico empleado y llega a todo tipo de personas.

Por añadidura debo recordar que el derecho penal no admite la analogía, entonces, ¿Estas acciones constituyen apología del delito o deben ser consideradas como un tipo aparte?

Si bien esto sucedió en algunas partes del mundo lo cierto es que no se ve tan frecuente pero podría contemplarse la opción de su incorporación como un delito informático. Este punto será retomado desde la óptica Española en el Capítulo de Derecho Comparado.

3.2 Análisis de la estructura del delito adecuada a la problemática

Cómo sostiene Zaffaroni: “no todo hecho que causa un resultado es una conducta humana, aunque sea una persona la que origina la causalidad, que desemboca ese resultado”. (Zaffaroni, 2005, p. 307)

Pero como parte de la teoría del Delito se encuentra la acción, la cual se debe conceptualizar para avanzar en esta estructura y justificar el porqué de la tipificación de estas conductas disvaliosas informáticas. La acción, conducta, o acto es el género del delito y su definición es la voluntad humana exteriorizada en el mundo. (2005, p.309).

“La función de la teoría del delito es analizar la acción humana delictiva, conforme a parámetros normativos y de acuerdo con un método construido por la dogmática.” (Donna, 2008, p. 173)

Donna entiende que: “el concepto de acción debe basarse en la idea esencial de que el hombre es el centro del problema penal; Y esto porque este es **nuestro** punto de partida: el respeto a la dignidad humana y a sus derechos fundamentales”. (Donna, 2008, p. 166). El autor también realiza un análisis sobre el injusto penal, que encuadra en su análisis dentro de la teoría del delito, pero que no viene al caso dada la idea que estoy tratando en este trabajo.

Como bien indica el Dr Zaffaroni la acción que forma parte de esta teoría del delito a su vez pertenece al derecho penal el cual debe brindar un concepto jurídico y en razón de la naturaleza no puede inventar una determinada cosa que no sucede en el mundo.

Siguiendo con esta línea de pensamiento podría argumentar que quizá hace veinte años atrás no consideraríamos estos delitos como posibles ya que no se verían en la realidad, ya que no formaría parte del accionar de esos sujetos en ese momento determinado. Pero como todo siguió su curso y el avance tecnológico surgió se dieron lugar a estas nuevas conductas que deben ser tipificadas.

Luego reflexionando acerca de los tipos se llega a la conclusión de que los mismos no pueden captar acciones privadas y esto es por determinados principios constitucionales que así lo establece. Dicho de otro modo las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Pero lo que sí puede ser alcanzado, o en palabras del autor, captables como prohibidas son

todas las que manifiestan sus efectos lesivos como obra de la gente, es por eso que los tipos captan la acción y su obra. (Zaffaroni, 2005, p. 315)

Respecto a la tipicidad se trata de dar un concepto lo más cercano posible para esto se dice que *“el tipo penal es la fórmula legal necesaria al poder punitivo para habilitar su ejercicio formal y al derecho penal para reducir las hipótesis de pragma conflictivo y para valorar limitativamente la prohibición penal de las acciones sometidas a decisión jurídica”*. (2005, pp. 336-337). Así continua sosteniendo que el tipo proporciona un ámbito máximo de prohibición que no puede exceder de alcance de las palabras pero que aun así es enorme y que si se considerase prohibido todo lo que cabe en el sentido literal de los tipos el poder punitivo sería demasiado grande.

Es por esto que al sostener la necesidad de tipificación de estas conductas destaque principalmente que se debe utilizar un lenguaje no tan limitado a una conducta en particular, sino a la utilización de un lenguaje un poco más abarcativo y que no se vuelva obsoleto de forma rápida; para que no pierda su utilidad y para que sea aplicado conforme las circunstancias.

Respecto al tipo de lenguaje que debe utilizarse en la redacción este debe ser de contenido un poco más amplio y no tan limitativo a una cuestión, como puede ser una red social ya que si el día de mañana desaparecen las redes sociales y aparece otra forma de comunicación por medio de internet o una tecnología similar al tipo; el mismo carecería de utilidad y sería necesario reformar el derecho penal de forma constante e incesante.

Demás está decir qué me refiero al “alcance de las palabras” cuando aludo al lenguaje no limitativo, o mejor dicho, a la utilización de palabras que no sean limitadas estrictamente a una cuestión.

Claro que no se pueden tipificar todas las alternativas es por eso que cuando puntualizaba sobre el “Spyware”, el “sextorsion” o el “spoofing”, este se entiende que es la denominación que la doctrina le ha asignado. Además el tipo comprende un supuesto de hecho y para poder alcanzar esto es necesario describir determinadas circunstancias que una vez que sean violadas por un sujeto el mismo sea susceptible de recibir una pena por parte del Estado, sin entrar en la discusión del fin de la pena; apuntando meramente a sintetizar la consecuencia jurídica que recaerá sobre el imputado.

El otro elemento que se debe analizar es la antijuridicidad, el autor citado sostiene que la antijuridicidad podría ser considerada como la otra cara de la libertad social, su otro lado, su opuesto, el cual está derivado del principio de reserva y esto lo afirma ya que sostiene que en un estado constitucional de derecho la regla es la libertad social y la excepción su limitación y por tanto la antijuridicidad sería la limitación a esa libertad social. (Zaffaroni, 2005, p. 458)

Al expedirse sobre el tema de la antijuridicidad o mejor dicho, sobre otro de los elementos de la estructura de la teoría del delito, el autor analiza en qué casos no habría antijuridicidad como puede ser la legítima defensa, la obediencia debida, entre otras.

Las causas de esta antijuridicidad no son relevantes para el análisis en cuestión ya que en principio no se aplicarían para esta clase de delitos y esto es porque no habría un estado de necesidad o una motivación fuera del sujeto que comete el hecho; la cual pueda ser inevitable para el mismo y esto sucede de esta forma porque esta clase de conductas tienen su origen en la intención de provocar un daño sobre determinados derechos personalísimos del sujeto; dado que el bien jurídico protegido de los mismos sería el derecho a la intimidad mayormente. También está incluida la afectación al patrimonio del sujeto; pero la norma vigente protege especialmente esta afectación.

Ya por último la culpabilidad es la “*actitud anímica jurídicamente reprochable del autor respecto de la consumación de un hecho penalmente típico y antijurídico*”. (Nuñez, 2009, p. 186). Acorde indica este autor, el reproche puede estar fundado en la imputabilidad, el dolo, la culpa y en la inexistencia de coacción.

Conforme a los hechos descriptos por este tipo estos delitos son cometidos a través del dolo ya que es un tanto complejo que los mismos puedan ser cometidos sin intención por parte del sujeto que los comete, o sea la comisión de estas conductas de forma culposa. Claro que debe analizarse cada caso en particular ya que no se puede generalizar la realidad misma.

Pero sin la intención de analizar cada texto que forma parte de la culpabilidad, en lo que se refiere a este tipo de conductas lo determinante es la voluntad que tiene el victimario para realizar estos delitos.

Distinto sería el caso de un homicidio ya que el mismo puede suceder de forma dolosa o culposa, puede haber un accidente de tránsito que origina lesiones gravísimas a una persona provocando su fallecimiento o puede haber una discusión y enfrentamiento entre dos cónyuges y que esto desencadene un homicidio agravado por

el vínculo. En estos dos escenarios se produce un homicidio en circunstancias distintas y con factores de la culpabilidad distintos como bien se observó, en primer lugar la culpa y luego el dolo.

Resultará motivo de prueba determinar si en estos delitos cabe la posibilidad según las circunstancias, de que se haya cometido con culpa del sujeto ya que si nos referimos al ámbito del revenge porn es muy difícil e improbable que se pueda sostener un actuar culposo por parte del sujeto al que se le imputa el hecho. Supongamos que se difunde un video privado de un sujeto con otro y este vídeo solamente lo tenía la víctima y el victimario intentará demostrar su culpa. Podría argumentar que el desconocía el origen del video, que nunca lo vio, que no le pertenece y la otra parte podría sostener que era un material que se encontraba solamente bajo su poder. Por supuesto que aquí caben todas las posibilidades de prueba como pueden ser las pericias informáticas que sean posibles en función de una autorización judicial, emanada de un juez competente. Como consideración final sería un tanto complicado prima facie que esto suceda por medio de la culpa o bien por medio del error ya que sería ilógico sostener que el error de una persona lo llevó a compartir de forma pública redes sociales un video íntimo de un tercero.

4. Pilares fundamentales que aspiran a la solución de la problemática.

Como he anticipado desde un comienzo, desarrollé una teoría y la misma se compone de supuestos presentes en la realidad.

Es común escuchar que una ley que describa conductas con el fin de tipificarlas resuelve conductas; bueno, esto no es así. Si bien a simple vista puede sonar contradictorio, lo que paso a concebir es una normativa penal integral abarcativa pero no solamente eso, y aquí entran en juego los pilares fundamentales en el derecho informático; los cuales tienen rasgos que no pueden ser empleados para otras ramas del derecho.

Entonces, ¿Qué es un pilar? Según la Real Academia Española, es un elemento estructural resistente, de sección poligonal o circular, con función de soporte; o bien una cosa que sostiene o en que se apoya algo. (Real Academia Española). Y es fundamental porque es a mí entender uno de los rasgos principales en este asunto. Pero, ¿Por qué estructuré de esta forma este punto, que función tiene?

Sencillamente mi aspiración es enseñar cuales son los pilares que sostienen la solución de “los delitos informáticos”; por esto mismo no me refiero solamente a un elemento como la norma penal.

La facilidad de encontrar una solución variada de distintos ejes es posible gracias a la Doctrina, la cual baraja distintas soluciones, algunos han sostenido que la Cooperación Internacional es elemental, otros sostienen que también lo es la normativa penal; por otro lado distintos expertos hacen alusión a la facilidad otorgada por la tecnología para la perseguibilidad de estos delitos. A mi parecer la composición de estos pilares forma la solución más idónea para encarar la problemática planteada al inicio.

Los cuatro pilares fundamentales sostienen a la solución: El primer pilar consiste en la normativa penal, el segundo en la utilización de tecnologías en el ámbito de la prevención e investigación de estos supuestos, el tercero de políticas activas por parte del Estado Nacional y el cuarto pilar, la Cooperación Internacional.

4.1 La normativa penal:

Es claro que al tratarse de conductas que se han ido denominando como “conductas disvaliosas informáticas” o tomando el permiso necesario “delitos informáticos”; se deja entre ver que, el que realice una acción será sancionado con la pena que merezca. Con base a esto se deberá establecer una pena proporcional, al hecho cometido y al perjuicio causado; por ningún motivo se podrá terminar utilizando como teoría la ley del talión; ya que irá en contra de los Derechos Humanos y significará un retroceso para la sociedad que si ha evolucionado, que sigue las normas y aspira al bien común. Sin intención de describir una utopía lo que transmito es claro, si se realiza una acción que vulnere uno o más derechos inherentes a la persona; se debe cumplir la sanción que el órgano legislativo haya plasmado, de forma previa al hecho; esto atiende a respetar el principio de irretroactividad que se maneja en el Derecho. Aquí planteo la primera característica, la proporcionalidad.

Por otro lado la situación actual ha llevado a la doctrina a señalar algo irrisorio en esta rama del derecho, por esto me refiero a la “analogía” que como bien se sabe no está permitida en el derecho penal. Y es que al encontrarse con situaciones derivadas de los delitos informáticos parte de la doctrina sugiere subsumir estas nuevas conductas a alguna norma que encuadre en líneas generales; pero de forma infructuosa, ya que al no otorgar especial tratamiento al hecho en cuestión se generan injusticias.

Del otro lado de esta corriente otros juristas sostienen que “*el delito informático requiere de la elaboración de respuestas normativas adecuadas en función de la inaplicabilidad de los tipos penales vigentes a las conductas disvaliosas descritas.*” (Altmark & Molina Quiroga, 2012, p. 144)

Así destacan que forman parte de la *dogmática penal* los principios como: *no hay delito sin pena (legalidad)*, o *el que prohíbe la aplicación extensiva de la normativa penal a una conducta analógica a la del tipo*. (Altmark & Molina Quiroga, 2012, p. 144).

Cabe aclarar que no se pretende sostener una regulación concreta de cada caso en particular ya que esto sería una tarea imposible e infinita, que hace impropio el objeto de la Ciencia Jurídica. Lo que si debe realizarse es la actualización de la norma, poner al día al derecho conforme a esta temática. Si alguna duda surge y versa sobre lo contrario a lo manifestado aquí; basta con observar que sistemáticamente planteo ir en contra de un *numerus clausus*, es decir, un numero cerrado de delitos informáticos; por esto planteo conductas disvaliosas que merecen tener una respuesta legislativa, tal como otros países tales como Estados Unidos, Brasil, España, entre otros; han adquirido.

Adhiero a la opinión del Dr. Marcelo Riquert en cuanto sostiene que: “*la asimilación con antiguas modalidades verbales sería una interpretación analógica contra el imputado y, por lo tanto, violatoria de la Constitución Nacional.*” (Riquert, Delitos informáticos en el anteproyecto del Código Penal de 2018, 2018, p. 17)

Siguiendo esta linea de pensamiento no me parece disparatado utilizar la analogía para el encuadre de una figura del derecho civil; donde la posibilidad de ubicar una situación en una norma puede ser manejada de mejor forma; pero en el derecho penal la analogía no respeta la proporcionalidad de la pena que corresponde para el caso en concreto; tampoco respeta el principio de la legalidad; sobre el cual me expedí en el presente capítulo.

Hasta aquí la normativa en cuestión debe responder a la proporcionalidad (conforme a lo explicado) y debe hacer caso omiso a la subsidiariedad de tipos penales. Además de esto la norma debe estar pensada de manera tal que permita ante la evolución de la informática; un tipo que no requiera actualización constante; a modo de ejemplo planteo la siguiente premisa:

Si la norma sanciona al que publique fotos o videos intimos de otra persona en una red social y luego la norma es sancionada; entra en vigencia y llegan casos para ser

investigados; a la hora de someter al autor al proceso penal no puede haber un impedimento generado por la norma, respecto a que en la misma se utiliza la terminología “red social” y se determina que el autor publico ese contenido en un sitio de internet que no encuadra en lo denominado “red social”.

El Dr. Fernandez Delpech expresa que se puede definir a las redes sociales como una *“plataforma de comunicación en Internet que permite a los usuarios interactuar a través del intercambio de datos personales comunes que facilitan la creación de redes”* (Fernández Delpech, 2016, p. 43)

Con lo cual si para ese caso hipotético se determina que el autor no estableció comunicación con ninguna persona sino solamente publicó el contenido en un sitio de internet que no encuadra en la definición aceptada para “red social”, lo que falla es la redacción normativa.

Ante estos casos se debe ser omnicomprensivo en la utilización de términos tecnológicos, sin que esto sea sinónimo de injusticia o arbitrariedad; sino de obtener una respuesta de acuerdo a la acción acontecida ya que no me refiero a un homicidio sino a conductas disvaliosas que se cometen en un medio muy versátil.

Entonces retomando la consigna de este eje, citaré un fragmento de texto elaborado por el *Consejo de Europa*, que se expide sobre la problemática tratada y el eje en cuestión; así considera que:

“La efectividad de la justicia penal es parte esencial de una estrategia de seguridad cibernética. Esto comprende la investigación, la fiscalización y la adjudicación de delitos en contra y por medio de datos y sistemas informáticos, al igual que la obtención de evidencia electrónica relacionada con cualquier delito, para propósitos del proceso penal. La naturaleza transnacional del delito cibernético y en particular la volatilidad de la evidencia electrónica implican que la justicia penal no puede ser efectiva sin una cooperación internacional eficiente. La legislación integral, que incluye el derecho sustantivo (la conducta a ser definida como delito) y el derecho procesal (los poderes investigativos para la aplicación de la ley), es fundamental para que tenga lugar la respuesta de la justicia penal. El consejo así considera que tal legislación debe cumplir con los siguientes requisitos:

- Debe ser lo suficientemente neutral (tecnológicamente) como para responder a la evolución constante del crimen y la tecnología, ya que de no ser así corre el peligro de volverse obsoleta para cuando entre en vigor. Esto es remarcado en todo

el trabajo; ya que al requerirse una normativa penal específica para esta problemática entiendo que debe tener la agilidad de mantenerse vigente por si misma; de ser autónoma; de no requerir una constante actualización por parte del legislador y lo elaborado en el marco del Consejo de Europa respalda dicha hipótesis.

- Los poderes para la aplicación de la ley deben estar sujetos a salvaguardias con el fin de garantizar el cumplimiento de los requerimientos del Estado de derecho y de los derechos humanos”. (Informe de ciberseguridad- Observatorio , 2016, p. 19)

4.2 La tecnología como una herramienta de prevención.

En primer lugar afirmo que el uso de programas de seguridad, que estén actualizados será vital para impedir vulneraciones en sistemas informaticos tanto de usuarios como de empresas. Emplear contraseñas seguras; no ingresar a sitios web fuera de los buscadores conocidos; cifrar las conversaciones con código, como permite whatsapp; entre otras. También realizar “back up” para tener toda la información almacenada en la Pc o teléfono resguardada.

Esto parecería inferir que el usuario es el único que puede tomar estas medidas; pues no; recientemente algunas empresas como Facebook y Youtube modificaron sus algoritmos para filtrar y en algunos casos eliminar contenido publicado allí mismo por ir en contra de sus políticas de uso; esto que parece abstracto se visualiza en el caso del “revenge porn” o los videos que han sido subido a youtube donde se copiaba un dibujo animado y se cambiaban los dialogos y escenas, siendo reemplazadas por contenido para adulto, lenguaje ofensivo, odio y violencia; con un destinatario claro, los niños.

Por otro lado en materia de delitos informáticos lo ideal sería sancionar transnacionalmente una norma que obligue a las empresas proveedoras de servicios (incluidas las redes sociales) para emplear medidas de seguridad informáticas; instruir a sus usuarios sobre como salir de un plano vulnerable en materia de seguridad informática; entre otras medidas que pueden sugerirse.

A parte se encuentra la propuesta donde el Estado a travez de una denuncia hecha por la victima de un delito informático pueda iniciar un proceso rápido para detener tales conductas reportadas y reunir prueba necesaria para juzgar a la persona. Es apropiado hacer hincapie en que no apunto a un espionaje, por el contrario me refiero a la actuación expedita por parte de una fiscalia que cuente con los técnicos informáticos que puedan resolver en breve tiempo el asunto.

Respecto a acceder a una red social o perfil digital o de internet del victimario a fin de detener las conductas y/o reunir prueba en su contra se debe realizar un análisis sobre el bien jurídico que tutela la figura y el que se sacrifica a raíz de la acción que se propone. Un elemento necesario es la orden de un juez que sustente la medida.

Cabe preguntarse si violaría la intimidad o bien se equipara a la justificación de violación de domicilio ante una orden judicial.

4.3 Políticas activas por parte del Estado.

El estado en primer lugar desde el poder legislativo debe impulsar normas tendientes a resolver este conflicto y otros tantos.

Será función entonces del Estado hacer publicas las leyes disponibles sobre delitos informáticos, ofrecer cursos de capacitación para informar a los usuarios sobre como estar protegidos en la red; así como informarles sobre los derechos que les asisten.

Otra tarea que le corresponde es resolver la situación actual de las fiscalías especializadas en delitos informáticos; acorde a la densidad poblacional y a las necesidades que puedan surgir en distintos espacios geográficos con un porcentaje mayor de habitantes. Actualmente hay tres fiscalías especializadas en estos delitos, las cuales cuentan con personal capacitado para atender temas de esta índole. Pero las mismas se ubican en la Ciudad de Buenos Aires; siendo que hay más territorio en el país y hay una cantidad mayor de ciudadanos que requieren especial atención a las vulneraciones que puedan sufrir en el Internet. Por esto, un sujeto que no pueda apersonarse a Ciudad de Buenos Aires o que en su localidad, provincia o partido no le informen sobre las fiscalías especializadas en estos asuntos; tendrá dificultado su acceso a la justicia; entendiéndose a la misma como un: *“principio básico del estado de derecho. Sin acceso a la justicia, las personas no pueden hacer oír su voz, ejercer sus derechos, hacer frente a la discriminación o hacer que rindan cuentas los encargados de la adopción de decisiones”* (ONU)

En palabras del Dr. Marcelo Temperini: Otro desafío sobre la investigación de este tipo de delitos consiste en la necesidad de cooperación de empresas privadas y proveedores de tecnología de información y comunicaciones con las autoridades policiales en la investigación criminal. Personalmente considero relevante la inclusión de esta observación realizada por el Dr. ya que si se quiere cubrir todos los espacios posibles para atacar la causa se deben considerar todos los aspectos. En relación con este tema él afirma que hasta el momento de la redacción de sus líneas no existe en Argentina una normativa que obligue a los proveedores de servicios de internet (ISP) a guardar las

direcciones IP asignadas a sus clientes por algún plazo determinado. En consecuencia, es posible que al realizar una investigación penal sobre algún hecho (y teniendo identificada la dirección IP del autor del delito) aun contando con la autorización judicial correspondiente no se pueda lograr identificar a la persona que la tenía asignada en un momento determinado, toda vez que algunas empresas no guardan dicha información o en el caso de guardarlas deciden no colaborar con la justicia. (Temperini, p. 68 y ss.)

En el capítulo 2 se analizara dentro del título: “Normativa penal en la actualidad” la resolución 977/19. Ya que es algo que debe ser mencionado.

4. 5 Una forma de Cooperación Internacional

La postura clave de un autor ya mencionado es la que utilizaré para ilustrar mejor esta noción, sin caer en la estricta concepción de creer que: “*Una nueva forma de cooperación internacional*” solo podría estar relacionado con conceptos del Derecho internacional privado. ***Aquí no se discutirán los grados de cooperación internacional sino las formas en las que se podría colaborar en la investigación, por ejemplo, de los delitos informáticos.***

Por la naturaleza transnacional del delito informático, los organismos internacionales intentan fortalecer la cooperación entre países no solo en materia de legislación penal, sino también en derecho procesal, la creación de organismos especializados y la asignación de facultades específicas para las autoridades de aplicación de la ley. Algunos problemas relacionados con la cooperación entre países en materia de delito informático son; la ausencia de consenso acerca de una definición jurídica de la conducta delictiva, la falta de conocimientos técnicos por parte de las autoridades de aplicación de la ley, la inadecuación de las facultades legales de investigación, la falta de armonización de los procedimientos de investigación y la ausencia de tratados de extradición y asistencia recíproca, entre otros. (Sain, 2013, p. 2)

Más allá de la tipificación de conductas ilícitas relacionadas con dispositivos informáticos y el fortalecimiento de la cooperación internacional en materia judicial y la existencia de organismos técnicos abocados a la seguridad informática, cada país debe tener una política pública en materia de ciberseguridad, una ley que regule el funcionamiento de internet en un determinado país y un organismo rector de aplicación abocado al desarrollo y regulación de la red dentro de su territorio. (Sain, 2018, p. 30)

Lo clave en materia de cooperación es repensar el concepto de evidencia y que el mismo abarque la evidencia digital, como señala Marcos G. Salt.

El punto mencionado ut supra es ubicado dentro de este pilar ya que si se piensa en un caso de esta magnitud que requiera solicitar datos a una empresa privada hoy sabemos, de buena tinta, que la mayoría de estas empresas son extranjeras; por lo que en el marco de la investigación de estos sucesos se debe requerir evidencia a empresas ubicadas en el extranjero. (Salt, 2017)

Como parte de este punto es clave destacar que Argentina forma parte del Convenio de Budapest por lo que habría un compromiso con la ciberseguridad en un plano transnacional. De igual forma este instrumento requiere ser ayornado por su época de redacción. Me expediré sobre este convenio en el siguiente capítulo.

Respecto al eje presente los Drs. Altmark y Quiroga se expiden sobre el Congreso de Viena sobre ciberseguridad en las naciones unidas; donde se enumeran los problemas existentes en la materia; los cuales que requerían la cooperación internacional respecto de los delitos informáticos:

1. *La ausencia de acuerdo sobre que conductas deben pasar a formar parte de la tipificación de delitos informáticos.*
2. *La falta de armonía en la definición legal de dichas conductas delictivas.*
3. *La escasa especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.*
4. *Ausencia de armonía entre leyes procesales nacionales sobre la investigación de estas conductas.*
5. *El carácter transnacional de estos delitos.*
6. *La carencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos concordados que permitan la puesta en vigor de la cooperación internacional*

Por lo tanto sostienen que al investigar los delitos informáticos, las autoridades encargadas de aplicar la ley de un Estado, pueden solicitar la cooperación de autoridades de otros Países, la misma cooperación puede consistir en asistencia o solicitar información sobre organizaciones y casos delictivos. Así mismo durante el desarrollo de la investigación pueden requerir se les facilite material, seguramente tecnológico pero que se encuentre en otros Estados. El alcance de la cooperación entre las autoridades nacionales encargadas de aplicar la ley viene determinado por acuerdos internacionales, incluidos acuerdos de asistencia judicial recíproca. (Altmark & Molina Quiroga, 2012, p. 169)

Los expertos participantes en la Convención de las Naciones Unidas afirmaron que los instrumentos jurídicos elaborados a nivel regional, en particular el Convenio del Consejo de Europa sobre la Ciberdelincuencia, “no eran una respuesta suficiente y que se necesitaba un instrumento jurídico elaborado mediante un proceso abierto y que estuviera abierto a la ratificación o adhesión universal bajo los auspicios de las Naciones Unidas. Sostuvieron que, dado el carácter mundial de las tecnologías de la información y las comunicaciones y del delito cibernético, resultaba esencial disponer de un instrumento jurídico universal, y señalaron que esos procesos e instrumentos no eran una novedad en la lucha contra las formas transnacionales de delincuencia”. (ONU, Estudio sobre el Delito Cibernético., 2017).

4.4 Cierre del capítulo.

Como mencioné en la hipótesis el crecimiento de los delitos informáticos fue en alza en los últimos años, desde la primera sanción normativa de los mismos se han originado nuevas conductas no contempladas en la actualidad por la norma penal.

Por esto es que no pueden brindarse estadísticas de las conductas nuevas pero si de las ya contempladas. Debe tenerse en cuenta que si todas estas se legislaran mañana mismo las denuncias próximas aumentarían notablemente lo cual no significa que la normativa haya empeorado la situación, sino que da lugar a que se tome conocimiento de la situación, lo que forma parte del primer paso para la solución. Una vez que se toma conocimiento los pilares fundamentales serán muy útiles, ya con una norma penal adaptada se empezará a dar seguimiento a los autores de dichas conductas para su investigación. Así mismo el empleo de las nuevas tecnologías y la educación por parte del Estado a todos los ciudadanos; además de la puesta en marcha de políticas activas generará la merma de las conductas descriptas.

El gran avance lo verán los ciudadanos al comprender que esos actos inmorales que realizan o padecen por fin tendrán atención normativa y habrá una justicia que este del lado de la víctima; sin afectar por supuesto las garantías del debido proceso de los eventuales imputados. Luego de esto se verá que en esta clase de conductas al tener un seguimiento activo del estado y al no haber ninguna necesidad que obligue al sujeto a cometer estas acciones, se reducirán los casos en donde esto surja.

Por último es destacable que toda vez que un grupo de conductas que van en aumento en distintas partes del territorio, que causan un daño a una o más personas vulnerando derechos personalísimos deben ser reguladas por el Estado a fin de garantizar el orden en la sociedad.

Capítulo 2- “Normativa penal en la actualidad”.

Como introducción a este segundo capítulo considero que se debe destacar la importancia en el análisis de la legislación actual. Durante el desarrollo del presente mostrare distintos tipos de normas algunas penales, como la ley n°26.388 y otras como Instrumentos Internacionales que fueron ratificados recientemente.

El objetivo es evidenciar el margen nulo para sancionar conductas como las que he descripto en el “Capítulo N° 1” y por otro lado proponer algunas alternativas para suplir ciertas falencias. Respecto a las conductas descriptas las mismas conforman un grupo de acciones disvaliosas que no son objeto de regulación por parte de la norma, las que afectan a la intimidad de los sujetos en la sociedad y no exclusivamente al ámbito patrimonial; ya que estos están contemplados actualmente.

Algunos de los *instrumentos* que se analizarán serán el marco para sostener la necesidad de normativa ante distintas situaciones y que es lo que implica la inexistencia de las mismas para eventuales víctimas.

Por un lado el análisis normativo tendrá su inicio con normas nacionales y luego con distintos instrumentos que Argentina ha incorporado a su sistema jurídico, como son los tratados que se han ratificado. Para luego examinar el Proyecto de reforma del Código Penal. El mismo parece cumplir de *mejor* forma con todos los compromisos a los que Argentina se ha comprometido al ratificar el Convenio de Budapest hace a penas algún par de años. Nótese que Argentina en principio cumpliría con parte de lo pactado en la Convención, la ley fue reformada en su momento; dejando situaciones fuera del marco legal pero pronunciándose parcialmente sobre lo requerido por allá en 2001, sobre la problemática. Lo cierto es que el Convenio de Budapest también debería ser pasible de una actualización conforme al paso del tiempo y las nuevas conductas que se originaron. Esto se analizará específicamente en el análisis del Convenio en cuestión; el cual formará parte de este capítulo.

Recientemente algunos países que están atrasados como la Argentina han adherido a este Convenio y esto es consecuencia de la multiplicación de situaciones que no están bajo la “vista” de la norma; es decir situaciones no previstas por el legislador pero que hoy están causando innumerables problemas. Lo destacable es el avance de la doctrina en este eje, ya que en nuestro país distintos especialistas en la materia han advertido de la vulnerabilidad informática que hay en el territorio por el retroceso normativo y que afecta todos los usuarios.

Ley N° 26.388 - ¿Desenlace del problema?

Esta ley que modificó el Código Penal fue pensada para cumplir con lo establecido por el Convenio de Budapest, otorgando así protección normativa respecto a alguno de los delitos informáticos pero que afectan al patrimonio de los particulares; toda vez que se vea afectado por la intervención de un tercero, mediante la utilización de manipulaciones informáticas para obtener datos o cualquier contenido susceptible de ser revelado y sacar un provecho económico. La única situación vinculada a la integridad sexual es lo referido a la pornografía infantil; lo cual es sumamente positivo que se haya incorporado en la legislación.

Lo criticado de esta ley es la infinidad de situaciones que no regula; empezando por olvidar u omitir la protección al bien jurídico de la intimidad. Sobre lo que si se ha expedido es sobre la privacidad entendiéndose esta como un concepto más general; pero olvidando los casos donde la intimidad del sujeto es vulnerada por un tercero. Esta norma sin embargo en su momento fue fruto de muchos halagos debido a que se pronunciaba sobre una cuestión tratada en el Convenio, pero desde entonces diversos especialistas pusieron su foco en ella y abrieron la discusión, la norma no regula distintas situaciones. Sin la intención de sacar conclusiones desmedidas dejo abierto al criterio personal el motivo al que esto atiende.

En un primer lugar hay que mencionar que la norma se destaca en cuanto a explicar en qué consisten algunos términos; es decir que adopta la misma metodología que en el Convenio de Budapest pero para definir términos distintos. Así la ley en cuestión establece que se entiende por:

1. Documento: Como una representación de actos con independencia del soporte utilizado para su almacenamiento. Esta aclaración sobre la independencia del soporte utilizado tiene injerencia directa sobre el tema en cuestión ya que permite comprender documentos en soporte papel y en soporte electrónico o digital.
2. La firma digital.
3. Por último añade que toda vez que en el Código Penal se lea: "instrumento privado" y "certificado" se entenderá por ello el documento digital que contenga una firma digital.

Por otro lado, la Convención define los siguientes términos:

1. Sistema informático.
2. Dato informático.
3. Proveedor de servicio.
4. Datos relativos al tráfico.

Los mismos serán analizados respectivamente bajo el título del Convenio; en el presente capítulo.

Además la norma impone una pena de seis meses a cuatro años a todo aquel que ***produzca, financie, ofrezca, comercie, publique, facilite, divulgue o distribuya***, por *cualquier medio* la representación de un menor de dieciocho años, referido a actividades sexuales o representación de sus partes genitales, con fines sexuales; al igual que el que organice espectáculos en vivo del mismo tipo de representaciones. Así disminuye la pena (de cuatro meses a dos años) para el que tenga en su poder esas representaciones con el fin de distribuirlo o comercializarlo. Y ya por último reduce la pena de un mes a tres años al que facilite el acceso al tipo de espectáculos ya descriptos o suministre material pornográfico a menores de catorce años.

Lo criticado en su momento, según A. Palazzi es que la norma no penaliza la simple tenencia de este material de índole sexual referido a menores de edad; es decir que la simple tenencia sin fines de distribución sería enmarcada dentro de la atipicidad. Reggiani (2008), citado en Palazzi, sostuvo que:

Ante la contundencia de los datos de la realidad, tales como el secuestro en allanamientos de grandes cantidades de material pornográfico destinado al intercambio o comercialización, el Congreso resolvió reprimir la conducta de tener en su poder representaciones de las descriptas anteriormente pero requirió en forma inequívoca en procura de salvaguarda del principio de reserva, la finalidad por parte del autor de proceder ulteriormente a su distribución o comercialización. (Palazzi, Los delitos informáticos en el Código penal, análisis de la ley 26388, 2016, pág. 32)

Ya en otra parte del articulado de la presente se hace referencia a la violación de secretos y privacidad, por la cual se penaliza al que *acceda, abra indebidamente una comunicación en soporte electrónico o de otra naturaleza*, que no le esté dirigido, o se apodere indebidamente de alguna comunicación aunque no esté cerrado; o suprima o desvíe de su destino una correspondencia electrónica o comunicación que no le esté dirigida. Se incluye en la pena establecida a la acción de esa naturaleza que recaiga sobre cualquier sistema privado o de acceso restringido.

Se penaliza también con distinta pena al que comunique a otro o bien publique el contenido de la comunicación. Por último incorpora la inhabilitación especial para el funcionario público que cometa un hecho de esta naturaleza.

Algo a elogiar de la norma explicada ut supra es que amplía el margen para las comunicaciones informáticas como puede ser el acceso a una cuenta de correo electrónico con los fines indicados anteriormente.

Las conductas alcanzadas incluyen:

- El acceso sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.
- el acceso en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.
- **Se multa a quien** hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.
- Al que violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; proporcionare o revelare a otro información registrada en un archivo o insertare o hiciere insertar datos en un archivo de datos personales.
- El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.
- El que vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.
- el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.
- La sustracción, alteración, destrucción en todo o en parte objetos destinados a servir de prueba ante la autoridad competente.

Enmendando una omisión, Ley N° 27.436.

Siendo aquellas las reformas introducidas en el Código Penal en razón de la ley 26.388 determinadas situaciones fueron omitidas por parte del legislador; esto es lo criticable. Antes de hacer referencia a esta ley, debe mencionarse la n° 26.904, sancionada en el año 2013 y donde se modifica el artículo 131 del Código Penal,

estableciendo que: será sancionado con una pena de seis meses a cuatro años al que por medio de comunicaciones electrónicas, o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma”. La pena para algunos autores debería ser menor y para otra parte de la doctrina la escala penal asignada es la adecuada. Lo cierto es que podría contemplarse como un delito de peligro abstracto.

A favor se argumenta que el fin del tipo es desalentar esta clase de conductas.

En materia de pornografía infantil en aquel momento fue un desacierto que no se contemplara dentro del tipo la simple tenencia. Esto fue mejorado por la ley 27.436 del pasado 2018; es decir que pasaron diez años hasta que la situación vio una mejora.

La ley 27.436 puso fin a la espera, penando la simple tenencia de pornografía infantil. Además de esto se formuló un agravante para estos delitos cuando la víctima fuera menor de trece años de edad. Y en un aspecto general se aumenta la escala penal para las conductas que describe.

Así estableció que será reprimido con prisión de cuatro meses a un año el que a sabiendas tuviere en su poder representaciones de las descriptas en el párrafo anterior.

Si bien es claro que la mayoría de la doctrina está a favor de esta penalización hay otros autores que se oponen a esto en virtud del principio de reserva derivado de la Carta Magna.

Así Marcelo A. Riquert citando a Martin Rico; este último estando en contra de la inclusión de esta figura y señala que “se estaría obedeciendo a lo nombrado en el art. 19 de la Constitución” y que estarían exceptuados de este nuevo tipo aquellos que naveguen en páginas que contienen pornografía infantil. (Riquert, 2019, p. 265)

En mi opinión es **desalentador** que se utilicen preceptos Constitucionales para avalar determinadas conductas inmorales que nada tienen que ver con la “moral sexual”.

Como bien anticipe la ley 26.388 que parecería denominarse: Ley de los delitos informáticos; sería una denominación un tanto “grande” para los tipos que comprende y los que omite. Ya habiendo expuesto las razones por las que esta norma es elogiada debo expedirme sobre las cuestiones que no contempló, sin saber cuál fue el motivo para esto.

En primer lugar el agravante en la escala penal para funcionarios públicos es aplicable solo en algunas conductas.

No ha introducido o adecuado el bien jurídico protegido, contemplando el contexto en el que nos encontramos, siendo este el de la sociedad de la comunicación y la abundancia de las redes sociales.

Así Carlos C. Sueiro señala que: nuestra ley tampoco ha contemplado la protección de un bien jurídico colectivo, macro social o supraindividual, como por ejemplo la protección del hipotético “ciberespacio público”, “medio ambiente digital” o “seguridad informática pública” en relación con lo lesivo que podría resultar para un importante número de bienes jurídicos tradicionales como la vida, la integridad física, la libertad, la propiedad, la seguridad pública, etc, el afectar mediante un ataque informático a todas las actividades públicas que dependen directa o indirectamente del correcto funcionamiento de sus sistemas informáticos públicos interconectados vía internet y también a través de intranet. (Sueiro, 2011)

Por otro lado las conductas mencionadas en el “Capítulo 1” han sido omitidas, a modo de síntesis y para evitar una repetición innecesaria me limitare a enumerarlas:

1. Ciberstalking.
2. Deepfakes.
3. Spyware.
4. Distribución, publicación, venta de Malware.
5. Sextorsión.
6. Spoofing.
7. Revengeporn.
8. Publicación o difusión por medio de internet, de contenido audiovisual

donde se observe la comisión de ilícitos.

Carlos C. Sueiro considera como una omisión de la normativa las siguientes conductas:

- 1) La ciberocupación o registro impropio de nombres de dominio
- 2) El Spamming o correo basura o publicidad no solicitada
- 3) La captación ilegal y difusión de datos, imágenes y sonidos
- 4) La posesión simple de material pornográfico infantil
- 5) La responsabilidad de los proveedores.

6) Que fue concebida únicamente como una ley sustantiva de reforma al Código Penal de la Nación en materia de criminalidad informática, sin ser acompañada por una reforma a nivel procesal.-

Respecto del segundo punto que menciona el autor podría objetar que el spamming difícilmente será considerado como un delito ya que es detectado por la

mayoría de los “filtros” que poseen los correos tales como Gmail, Yahoo, etc. Es decir que la problemática que plantea es de cuestionable tratamiento. Por otro lado entiendo que el spamming en algunas ocasiones tiene por fin la defraudación o la estafa; allí la situación podría ser distinta porque estaríamos ante una estafa por medios informáticos. La mejor solución sería establecer un precepto general de estafa o defraudación informático y no solo limitarlo al “envío de correos” ya que esto limitaría el ámbito en el que pueda pensarse y obviaría nuevamente distintas acciones que deberían estar comprendidas.

El tercer punto mencionado fue objeto de tratamiento por mi parte, pero tomando como bien jurídico protegido a la intimidad sexual. Sobre la captación de datos en particular si se hace referencia a las disposiciones de la ley 25.873 y de su dec. regl. 1563/2004 esto es sumamente relevante ya que se vulneran los derechos consagrados por la Carta Magna en los arts. 18 y 19, dado que la ley en cuestión autoriza la intervención de las comunicaciones telefónicas y por Internet sin especificar las situaciones en las que esto puede producirse. Es por esto que referirse a la “captación ilegal y difusión de datos imágenes y sonidos” es un tanto amplio y debió haber sido objeto de más desarrollo con el fin de delimitar su contenido y averiguar si es pasible del tratamiento legislativo. En los casos mencionados por mi parte entiendo que si son susceptibles; esto es: cuando la intimidad sexual debe ser protegida y cuando se vulneran los arts. 18 y 19 de la Constitución en virtud de una ley de carácter Inconstitucional, como lo es la mencionada anteriormente.

Sobre el cuarto punto recientemente en el año 2018 la ley N° 27.436 suplió las falencias mencionadas, pero el autor menciona este punto ya que su publicación es anterior a la reforma.

Sobre la responsabilidad de los proveedores:

Este punto en cuestión merece un análisis a parte. Cuando se refiere a la responsabilidad de los proveedores lo hace exclusivamente a los: “ISP” Internet service provider; es decir proveedores de servicio de internet.

Hoy en día la comunicación está integrada por estos intermediarios denominados ISP o PSI en su traducción al Español. Hasta aquí no hay ninguna discusión que se presente; pero si se analizan las distintas teorías y propuestas contra los delitos informáticos algunos proponen (como es el caso del autor mencionado anteriormente) legislar sobre la responsabilidad que atañe a estos intermediarios.

A simple vista la cuestión no parece tan controversial; es decir imputar responsabilidad a un intermediario por lo que suceda bajo su “control”; el asunto clave aquí es que siendo tantos los usuarios que comparten contenido en internet es un tanto difícil controlar que es lo que circula a través de la red. Aquí nuevamente se presenta otro tema a discutir, ya un poco más en profundidad parecería sugerirse espiar a los usuarios para determinar qué tipo de contenido están compartiendo o haciendo circular.

Ahora bien es evidente que pretender atribuir responsabilidad legal a estos intermediarios por el contenido las comunicaciones implica una vulneración para los usuarios, específicamente el derecho a la privacidad que estos tienen y por qué no la libertad de expresión.

Con el fin de explicar un tanto mejor en que consiste esta idea, citare el artículo: “Principios de Manila”, un artículo de España brindado por una organización de sociedad civil.

En el mismo se discute en un primer lugar que debe haber una regulación legal para la protección de un sujeto en particular, los intermediarios; es decir que deben gozar de una protección legal contra la responsabilidad por los contenidos de terceros y esto es algo fundamental ya que cada sujeto tiene total autonomía sobre sus acciones y no puede atribuírsele responsabilidad (en principio) a un simple intermediario; el cual tampoco está facultado para intervenir en las comunicaciones de esos usuarios por ser violatorio de la privacidad. Por eso el que debe ser sancionado en el caso que corresponda es ese usuario que cometa conductas disvaliosas y en todo caso se puede requerir el auxilio de una ISP con el objeto de reunir prueba suficiente para la investigación de los hechos.

Así los citados principios explican que:

1. Toda disposición destinada a regular la responsabilidad de intermediarios debe ser establecida por una ley preferentemente de redacción precisa y clara.
2. No puede atribuirse responsabilidad por el contenido de terceros siempre que no hayan estado involucrados en la modificación del mismo.
3. Los intermediarios no deben ser responsabilizados por no restringir contenido lícito. d. Tampoco deben tener responsabilidad objetiva por alojar contenido ilícito de terceros, ni mucho menos controlar la actividad de los usuarios.
4. No debe requerirse la restricción de contenidos sin una orden emitida por una autoridad judicial es decir que el principio es la libertad de expresión y la excepción

es la orden judicial emitida por una autoridad competente, la cual haya sido dictada en función de que el contenido en cuestión es ilícito.

5. “Las órdenes de restricción de contenido deben: Explicitar la determinación de que el contenido es ilícito en la jurisdicción, a su vez indicar el identificador de Internet y la descripción dicho contenido; proporcionar evidencia suficiente para documentar el sustento legal de la orden y de ser aplicable, indicar el período de tiempo durante el cual el contenido debería ser restringido.” Entiendo que este punto es relevante pero tampoco puede interferir en las cuestiones procesales del ordenamiento jurídico en que esto se presente.

6. Si se atribuye algún tipo de responsabilidad sobre un intermediario debe ser proporcional al comportamiento ilícito del intermediario de no cumplir adecuadamente la orden de restricción del contenido.

7. Por último añaden que no deben ser responsabilizados por el incumplimiento de cualquier orden que no cumpla con el punto cinco.

Como pautas generales recomiendan que los gobiernos deban publicar en Internet toda legislación, que sea relevante respecto de la responsabilidad de los intermediarios en formatos accesibles.

Que los Estados no deben utilizar medios extrajudiciales para restringir contenido. Que los mismos deben publicar informes de transparencia que brinden información sobre todas las órdenes y requerimientos solicitadas por ellos ante los intermediarios, también publicar informes que proporcionen información acerca de todas las restricciones de contenido adoptadas por el intermediario. Y por último que los marcos y legislación sobre responsabilidad de intermediarios deberían estar sometidos a una revisión constante para asegurar que no estén desactualizadas, para promover su eficacia y que la revisión periódica debería incorporar mecanismos de recolección de evidencia acerca de su implementación. (Principios de Manila, 2015)

Todos estos principios detallados ***son meras sugerencias brindadas por una organización Española***, lo cual no debe dejarse de lado; por lo tanto esto se incorpora a fin de tener un marco de referencia sobre cómo deberían ser las normas sobre las ISP.

Jurisprudencia vinculada.

No habrá posibilidad de incorporar jurisprudencia distinta a la explicada en el siguiente acápite ya que al no estar legisladas las conductas planteadas, no habrá jurisprudencia a tal fin. Es por esto que lo más similar es un caso de daños y perjuicios donde aparece este nuevo problema en la esfera jurídica.

Rodríguez María Belén c/ Google.

Sobre este tema en particular se deben mencionar los autos "Rodríguez, María Belén c/ Google Inc. s/ daños y perjuicios", que data del 2014. Del fallo surge que la actora interpuso la demanda por daños y perjuicios contra Google Inc. (Google) - después la misma fue ampliada contra Yahoo de Argentina SRL (Yahoo). En ella se sostiene que se había procedido al uso comercial y no autorizado de su imagen y que vio sus derechos personalísimos afectados al habérsela vinculado a determinadas páginas de Internet de contenido erótico y/o pornográfico. Pidió también el cese del mencionado uso y la eliminación de las vinculaciones.

La sentencia de primera instancia hizo lugar al pedido de la demandada y dictaminó que las empresas demandadas habían incurrido en negligencia culpable "al no impedir la existencia de contenidos nocivos o ilegales perjudiciales a los derechos personalísimos de la actora, a partir de serles comunicada la circunstancia". Por lo expuesto condenó a Google y a Yahoo a dar distintas sumas de dinero como así, de disponer la eliminación de las vinculaciones del nombre, imagen y fotografías de la actora.

Luego del fallo de primera instancia las partes apelan la resolución y la Cámara Nacional de apelaciones en lo Civil resuelve: revocar parcialmente la decisión de primera instancia; así revoca el reclamo contra Yahoo y admite el interpuesto a Google, pero reduciendo la suma de dinero que este debía dar; por lo que la Cámara A entendió que correspondía el reclamo solamente contra Google por encuadrar la eventual responsabilidad en la esfera subjetiva. Sobre la negligencia se pronuncia rechazándola debido a que la actora no intimó extrajudicialmente a las empresas demandadas sino que se limitó a obtener una cautelar.

Se interpone recurso extraordinario y la Corte resuelve:

Que hay casos en que el buscador puede llegar a responder por un contenido que le es ajeno y ello sucederá cuando haya tomado efectivo conocimiento de la ilicitud de ese contenido, si tal conocimiento no fue seguido de un actuar diligente.

La Corte entendió que no correspondía aplicar la Ley 11.723 ya que no se juzgaba la responsabilidad que podría atribuirse a una página de Internet, por la indebida publicación o reproducción de imágenes, sino a un mero intermediario cuya única función es servir de enlace con aquella. Por último la corte dictaminó que toda restricción, sanción o limitación a la libertad de expresión debe ser interpretada en forma restrictiva, y que toda censura previa que sobre ella se ejerza padece una fuerte

presunción de inconstitucionalidad; con lo cual, teniendo en cuenta las constancias de autos, determinó que la tutela preventiva no resulta aplicable, toda vez que no se ha invocado un caso que justifique apartarse de los principios ya sentados por la Corte al respecto.

Así por todo lo mencionado el recurso extraordinario de la actora fue rechazado y se hizo lugar al deducido por Google, revocando parcialmente la sentencia apelada.

Disidencias:

Dres. Lorenzetti y Maqueda, respecto de dos puntos tratados a lo largo de la sentencia dictada.

Así consideraron que resulta aplicable el artículo 31 de la Ley 11.723 sobre “thumbnails”, toda vez que a través de ellos los buscadores utilizan, almacenan y reproducen, mediante una copia reducida, imágenes publicadas por terceros, con la posibilidad de ser descargas o impresas desde el sitio web de “Google”.

Ahora bien, sobre la eliminación del contenido que la vincula provocando una afectación al nombre, imagen, honor e intimidad de la actora, interpretan que lo que se pretende a través de la vía intentada es una tutela judicial de un derecho personalísimo a su vez compatible con la libertad de expresión. Consideran entonces admisible lo solicitado siempre que se identifique cuáles son los enlaces asociados a su persona y se compruebe el daño que la vinculación ocasiona. (Rodríguez c/ Google inc. s/ Daños y perj., 2014)

Conclusión: El fallo Rodríguez versa sobre la responsabilidad de los intermediarios, específicamente sobre los proveedores de servicio de internet y el “rol” amplio que podrían ocupar en el marco de los delitos informáticos.

En primer lugar es de carácter notorio que al no estar tipificada esta “responsabilidad” determinada se ha interpuesto una demanda y no una denuncia. La opinión de la Corte no debe dejarse de lado toda vez que se proponga atribuir responsabilidad a algún miembro de la cadena de ISP.

Por mi parte sostengo que establecer responsabilidades para los ISP no garantiza la prevención de las conductas. El proveedor de servicios no puede ser responsable por los actos que desee realizar el usuario. En el hipotético caso de que el proveedor tenga la obligación de “controlar” la actividad que el usuario tiene en internet considero que se estaría vulnerando el derecho a la privacidad que todos tenemos;

distinto sería que se investiguen los actos de un usuario previa denuncia de la víctima y se refieran a actos específicos y no a toda la actividad que el sujeto “desplega” en Internet.

Parte de la doctrina sostiene que la mayoría de los casos no existe responsabilidad para los ISP ya que razones generalmente tecnológicas les impiden ejercer un control permanente de los contenidos de terceros que transmiten o alojan, dado a la imposibilidad de controlar, por la cantidad, la información que se encontraba en el servidor. Además, obligarlos a eliminar o bloquear contenidos que creen ilícitos, implicaría ni más ni menos que legalizar la privatización de la censura, toda vez que los ISP, fuera de los casos de contenidos manifiestamente ilícitos, serían quienes disciernen si un contenido es lícito o ilícito, si es nocivo o no. (Martínez & Porcelli, p. 134)

Para finalizar debo aclarar que este análisis se realizó porque hay parte de la doctrina como la mencionada que sostiene como una posible solución a los delitos informáticos la atribución de responsabilidad para los intermediarios; por mi parte considero que la solución oportuna consiste en los cuatro pilares fundamentales, teoría que explique en el Primer capítulo del presente trabajo.

A propósito de esta idea debe destacarse que hay un proyecto de ley para **limitar** la responsabilidad de los intermediarios, el cual tiene media sanción del senado (S-1865/15).

Lo correcto sería primero poder sancionar el anteproyecto del Código Penal y luego sancionar el nombrado proyecto de ley, ya que si ocurre de forma inversa las víctimas de determinadas conductas disvaliosas se verán aún más desprotegidas; ya que si no hay una norma penal que establezca la tipicidad de ciertas conductas como el “Revenge porn”, “sextorsion”, la suplantación de identidad digital, o los “Deep fakes”; lo único que se lograra es sancionar una ley que exponga más a las víctimas y no otorgue herramientas concretas para obtener justicia.

Ley de datos personales, N° 25.326

La ley en cuestión define como dato personal a toda información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

El objeto de la norma es brindar protección a los datos personales presentes en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que

sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.

En la misma ley se brindan algunas definiciones, las cuales solo serán nombradas:

- Datos informatizados
- Archivo, registro, base o banco de datos.
- Tratamiento de datos, responsable de archivo, registro, base o banco de datos, titular de los datos y usuario de datos.

La misma ley regula otras conductas sobre, como se recoleccionan los datos personales, de qué modo deben almacenarse, cuestiones especiales sobre el consentimiento para su obtención, entre otras cosas, a saber:

- La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.

- Y aquellos datos no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

- Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario.

- Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular. Los mismos deberán ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

- El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.

- Ninguna persona puede ser obligada a proporcionar datos sensibles.

Sobre el consentimiento establece que, en los siguientes casos no será necesario:

- Los datos se obtengan de fuentes de acceso público irrestricto;
- Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;
- Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;

- Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;
- Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526.

Por último, sobre excepciones, se determinó que la transferencia internacional de los mismos está prohibida a excepción de:

1. Casos de colaboración judicial internacional
2. Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica
3. Transferencias bancarias o bursátiles
4. Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte
5. Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

Como parte de los derechos que le asisten a los titulares se establece: El derecho de rectificación, actualización y, cuando corresponda, de los datos personales de los que sea titular, que estén incluidos en un banco de datos.

La excepción a los derechos mencionados: Se puede, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros. Como así también cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado.

El escenario normativo luego de la ley N° 26.388:

La sanción que establecía la ley presente fue derogada por la 26.388. Así finalmente se determina que: Se reprime con la pena de prisión de un mes a dos años el que a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; como al que ilegítimamente proporcionare o revelare a otro información registrada en un archivo o

en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley. También al que ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Y se agrava para el caso de funcionario público, determinando su inhabilitación especial.

Luego de haber expuesto lo principal que establece la ley de protección de datos, me parece necesario reflexionar sobre la distinción con el derecho a la privacidad de las personas. Para esto citaré al Dr. Pablo Palazzi, el mismo determina que el derecho a la privacidad es: *“Una instancia más evolucionada respecto a la protección de datos personales, es una respuesta a las necesidades del individuo que la exclusión de terceros con la reserva que otorga “el derecho a estar solos”*. Una crítica que realiza el autor a la ley en cuestión es sobre la venta de datos, la cual no ha sido contemplada como un delito. (Palazzi, Delitos contra la intimidad informática, 2019, pp. 271-273)

A tal fin elogio la ley en cuestión pero la misma **no resulta suficiente** para detener la problemática planteada en la hipótesis del trabajo.

El Anteproyecto del Código Penal de 2019

Por medio del decreto 103/2017 se crea la Comisión para la reforma del Código Penal de la Nación. Dentro de los “Considerando” se encuentran algunas líneas de interés para este trabajo, a saber:

“Que dicha tarea deberá tener en consideración, por un lado, los instrumentos internacionales de derechos humanos con jerarquía constitucional, en los términos del artículo 75 inciso 22 de la Constitución Nacional, y por otro los avances en materia de integración regional del país, favoreciendo la armonización de la legislación en sus aspectos fundamentales a fin de promover y facilitar la cooperación entre Estados y la implementación de estrategias coordinadas, elementos de máxima importancia ante ciertas modalidades delictivas como la delincuencia transnacional organizada.

Que de igual manera, resulta imprescindible que la normativa punitiva nacional sea adecuada a los compromisos asumidos en el plano internacional, en particular en lo atinente a la vigencia de la protección de los derechos humanos...”. Se debe realizar un llamado de atención y recordar que a fines del año 2017 Argentina se adhiere al Convenio de Budapest; el cual al ser un tratado internacional tiene jerarquía supralegal; por eso mismo Argentina debe cumplir con todos los aspectos de este Instrumento.

Por otro lado cabe aclarar que esto es algo que no se ha logrado aún pero que el anteproyecto en cuestión viene a subsanar tal falta. Respecto a delitos informáticos recientemente se ha subsanado la omisión de la ley 26.388 (la cual no penaba la mera tenencia de material pornográfico infantil) la que fue remediada posteriormente por la ley 27.436.

Otrosí en el 2019 el PEN remite el proyecto de ley PE 52/19, sobre la reforma del Código Penal.

Dentro del Título XXVI denominado “Delitos informáticos se contemplan distintas situaciones que se pasaran a analizar.

El artículo 491 establece que: se impondrá prisión de seis meses a dos años o seis a veinticuatro días-multa, al que ilegítimamente con **ánimo de lucro o la finalidad de cometer un delito**, y valiéndose de **alguna manipulación informática, ardid o engaño, obtuviere claves o datos personales, financieros o confidenciales de un tercero**, siempre que el hecho no constituya un delito más severamente penado.

La **misma pena se impondrá a quien compilare, vendiere, intercambiare u ofreciere, de cualquier manera, claves o datos de los mencionados en el primer párrafo**. La pena será de prisión de uno a tres años, en cualquiera de los casos de este artículo, cuando se tratare de un organismo público estatal.

El artículo tiene varias características eficaces ya que se intenta proteger el carácter privado de los datos personales ante amenazas de terceros, sea meramente con el fin de obtenerlos o bien de intercambiar, vender o compilar los mismos. Por otro lado sería oportuno preguntarse si cabe la misma pena para el que obtenga esos datos y al que posteriormente los ofrezca o venda. Por mi parte considero que debería ser más severa la pena de quien vende esos datos ya que primero los obtiene y luego lucra con ellos; y cabe recordar que según el primer párrafo es delito obtenerlos (con ánimo de lucro o la intención de cometer un delito) por lo que si además de eso se intenta lucrar con los mismos la pena que le pertenecería debería ser mayor.

El artículo 492 ordena que se imponga prisión de seis meses a dos años o seis a veinticuatro días-multa, al que a través de Internet, redes sociales, cualquier sistema informático o medio de comunicación, **adoptare, creare**, se apropiare o utilizare la identidad de una persona física o jurídica que no le pertenezca, con la intención de **cometer un delito o causar un perjuicio** a la persona cuya identidad se suplanta o a terceros. *Lo positivo de este artículo es que especifica la acción que comprende la*

normativa y se observa que se ha hecho un esfuerzo en su redacción para que la norma no se vuelva obsoleta rápidamente y queden acciones no comprendidas por el avance tecnológico. Es por esto que establece que es una conducta que puede cometerse mediante redes sociales o cualquier sistema informático o medio de comunicación.

Las palabras en “negrita” las considero las más relevantes de ese articulado; esto es por los conocidos “deepfakes”; videos editados y creados con inteligencia artificial que incorporan personas reales en situaciones falsas, son nuevas conductas informáticas donde por ejemplo se toma la imagen de una persona y se la inserta en un video imputándole a la misma el contenido de dicho video, es otra forma más moderna de suplantar la identidad de una o más personas que con el avance tecnológico está siendo posible. Por eso es tan relevante que se tomen medidas suficientes no solo para sancionar estos hechos sino para prevenirlos. Como bien menciono en “los cuatro pilares fundamentales” se deben tomar medidas no solo desde el Estado sino a través de la Cooperación, desde el plano Internacional y desde el ámbito público- privado. Es claro que si el material visual o audiovisual no ofende a ningún sujeto no debe ser susceptible de sanción alguna, pero en el caso de generar un daño debería ser alcanzado; lo cual esta detallado en la norma y a mi entender es altamente efectivo.

Dentro de las noticias, concretamente en un Diario de Uruguay, trasciende que Amazon se unió a Facebook y Microsoft para combatir este problema a través de un algoritmo, en el que se invertiría cerca de un millón de dólares. (“El observador”, 2019)

El artículo 493 dispone que se impondrá prisión de seis meses a dos años o seis a veinticuatro días-multa, al que sin autorización de la persona afectada difundiere, revelare, distribuyere o de cualquier otro modo pusiere a disposición de terceros imágenes o grabaciones de audio o audiovisuales de naturaleza sexual, producidas en un ámbito de intimidad, que el autor hubiera **recibido u obtenido con el consentimiento de la persona afectada**, si la divulgación menoscabare gravemente su privacidad. La pena será de prisión de uno a tres años:

1º) Si el hecho se cometiere por persona que esté o haya estado unida a la víctima por matrimonio, unión convivencial o similar relación de afectividad, aun sin convivencia.

2º) Si la persona afectada fuere una persona menor de edad.

3º) Si el hecho se cometiere con fin de lucro.

Conforme el artículo 72 inc 3° del anteproyecto serán acciones dependientes de instancia privada. Este artículo se ha esperado desde hace algunos años por parte de la sociedad, ya que conductas como estas no están alcanzadas por la ley penal y parecía que jamás iban a ser contempladas, hasta este momento, donde se plantea incorporarlas de lleno al nuevo Código. Si bien la redacción es clara pasaré a explicarla y a detallar que es lo que reprocho del articulado. Se plantea una pena benévola para los casos donde un sujeto obtiene por parte de otro material “sensible e íntimo” y se pena a todo aquel que la obtenga y distribuya o comparta con terceros. En resumidas cuentas cuando hay consentimiento para grabar tales imágenes y/o videos o bien cuando estos son puestos a disposición de un tercero.

Por lo tanto aquí hay dos hipótesis de tipificación:

- 1) Un sujeto obtiene o recibe **con el consentimiento** de otro, material sensible.*
- 2) Un sujeto lo distribuye, revela o envía **sin el consentimiento**.*

Es de carácter manifiesto que no se contempla que la hipótesis N° 1 suceda sin el consentimiento de la otra parte, lo cual debería ser alcanzado también por la normativa, justamente por la magnitud de lo que comprende tal acto. Esto es lo que recrimino del citado artículo ya que es una cuestión que también debe encontrarse comprendida por parte de la legislación.

Por otro lado en el “Capítulo II”, se incorpora el “daño informático”.

El artículo 494 establece que se impondrá prisión de quince días a un año o uno a doce días-multa, al que ilegítimamente y sin autorización de su titular alterar, destruyere o inutilizare datos, documentos, programas, sistemas informáticos o registros informáticos de cualquier índole. Si los datos, documentos o programas afectados fueren aquellos protegidos por la Ley N° 24.766, la escala penal prevista se elevará en un tercio del mínimo y del máximo.

Aquí a diferencia del artículo anterior cambia la pena. Agregándose la multa, y cambia la tipificación sugerida en cuanto se añade la falta de autorización del titular para configurar el tipo penal, además de su obtención ilegítima.

- **Artículo 183 CPN.** - Será reprimido con prisión de quince días a un año, (...)el que alterar, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

El citado artículo incluye además en su segundo párrafo una cuestión que es tratada de forma autónoma en el anteproyecto, conforme el artículo 498. Dentro de la redacción de estos artículos no se observan grandes diferencias, excepto por la incorporación de multas.

El artículo 495 dispone que la pena sea de prisión de tres meses a cuatro años:

1. Si el hecho se ejecutare en documentos, programas o sistemas informáticos públicos.
2. Si el hecho se cometiere en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.
3. Si el daño recayere sobre un bien perteneciente al patrimonio cultural de la Nación Argentina o de un Estado extranjero.

Se observa su esencia en el artículo 184 (...) Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

El artículo 496 dispone que la pena será de prisión de uno a cinco años si, por el modo de comisión:

1º) El hecho hubiere afectado a un número indiscriminado de sistemas informáticos.

2º) El hecho hubiere afectado el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad.

3º) El hecho hubiere creado una situación de peligro grave para la sociedad.

El artículo 497 determina que se le impondrá prisión de uno a cinco años, al que ilegítimamente y sin autorización de su titular, mediante cualquier artificio tecnológico, mecanismo de cifrado o programas maliciosos, obstaculizare o interrumpiere el funcionamiento de un sistema informático ajeno o **impida a los legítimos usuarios el acceso a los datos del sistema**, siempre que el hecho no importe un delito más severamente penado.

El artículo 498 ordena imponer prisión de quince días a un año o uno a doce días-multa, al que vendiere, distribuyere, hiciera circular o introdujere en un sistema informático cualquier programa destinado a causar daños.

Los citados artículos 496, 497 y 498 tienen una relación muy estrecha en cuanto a sus implicancias. Ambos son una novedad al ser contemplados por el

legislador especialmente el último numerado, por ejemplo a raíz de los conocidos “ransomware”, que son virus implantados generalmente a largas distancias físicas, destinados a buscar archivos con valor para la víctima y luego pedir rescate por ellos, entendiéndose que se priva de tal acceso a su titular, la víctima.⁸ Otros de estos virus llega en forma de notificación, mail, publicidad, etc. con la apariencia de una aplicación oficial (a modo de ejemplo) donde se piden ciertos datos a la víctima o bien por el solo hecho de “clickear” un enlace puesto a disposición de la misma y así se infecta toda su computadora, provocando un “secuestro de sus datos o la privación en el uso de esa computadora” con el objetivo de apoderarse de datos y/o obtener un beneficio económico con la condición de dejar sin efecto el bloqueo. (Info technology, 2017)

Es de conocimiento que hace poco tiempo un pueblo del centro del Estado de Nueva York en Estados Unidos, en el año 2015 fue noticia por haber admitido pagar un rescate para poder seguir utilizando sus computadoras. (BBC, 2015). Esto implica que los secuestros a dispositivos informáticos pueden ser padecidos por cualquier persona.

Por otro lado en el 2019 ha surgido una nueva noticia vinculada, donde se utiliza un “Stalkerware”, siendo la combinación terminológica entre Stalker: Acosador y Ransomware; el cual permite a través de manipulaciones informáticas intervenir y espiar todo el contenido multimedia que puede existir en el teléfono de una persona; siendo utilizado para espiarse entre parejas. (BBC, 2019). Pero esto, lógicamente, al no ser una “condición de uso” en la aplicación, puede ser utilizado contra desconocidos e inclusive padecido por cualquier persona.

En Mayo del 2019 también se ha conocido que un grupo de hackers ha “secuestrado” una ciudad entera de EEUU por más de dos semanas, el hecho tuvo lugar en Baltimore, donde unos ciberdelincuentes han infectado con un peligroso ransomware para pedir a cambio de “levantar el secuestro” la suma de cien mil euros.⁵⁸ Recientemente también ha sido noticia que estos tipos de ransomware se extienden a los celulares. (ABC- España, 2019)

“Capítulo 3” “Hurto y fraude informáticos”

El artículo 499.- Se impondrá prisión de un mes a dos años, al que, **violando medidas de seguridad**, ilegítimamente se apoderare o copiare información contenida en dispositivos o sistemas informáticos ajenos que no esté disponible públicamente y que tengan valor comercial para su titular o para terceros.

El artículo 500.- Se impondrá prisión de un mes a seis años, al que **defraudare** a otro mediante la introducción, alteración, borrado o supresión de datos de un sistema informático, o utilizando cualquier técnica de manipulación informática **que altere el normal funcionamiento de un sistema informático** o la transmisión de datos.

El citado artículo tendiente a regular la defraudación informática es actualmente contemplado de forma similar en el CPN, pero su tipo es más acotado respecto a las técnicas por las que puede llevarse a cabo. Quizá podría contemplarse que el tipo no incluya dentro de su verbo el “alterar” el normal funcionamiento, ya que la alteración, borrado o supresión de dato o puede ser realizada por una técnica no muy compleja que no altera el normal funcionamiento de ese sistema informático.

La comparación del texto citado anteriormente es producto del actual artículo 173.- Sin perjuicio de la disposición general del artículo precedente, se

Considerarán casos especiales de defraudación y sufrirán la pena que él establece: Inciso 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

El citado artículo tendiente a regular la defraudación informática es actualmente contemplado de forma similar en el CPN, pero su tipo es más acotado respecto a las técnicas por las que puede llevarse a cabo. Quizá podría contemplarse que el tipo no incluya dentro de su verbo el “alterar” el normal funcionamiento, ya que la alteración, borrado o supresión de datos quizá es realizada por una técnica no muy compleja que no altera el normal funcionamiento de ese sistema informático.

La comparación del texto citado anteriormente es producto del actual artículo 173.- Sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece: Inciso 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

“Capítulo 4” “Acceso ilegítimo”

El artículo 501 establece que se impondrá prisión de quince días a seis meses, si no resultare un delito más severamente penado, al que a sabiendas accediere por cualquier medio, sin autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

El artículo 73 inc. 2° del anteproyecto lo excluye de las acciones privadas a este delito. Este artículo es el mismo que el 153 bis del CPN.

El artículo 157 bis. hoy es producto de una mixtura de los arts. Del ante proyecto 499-500-501, a saber: Será reprimido con la pena de prisión de un un mes a dos años, el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
2. Proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.
3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años.

El artículo 502 dispone que la pena será de seis meses a dos años de prisión:

- 1º) Si el hecho hubiere afectado un sistema o dato informático de un organismo público estatal.
- 2º) Si el acceso hubiere afectado un sistema o dato informático de un proveedor de servicios públicos, de salud o financieros.
- 3º) Si el hecho hubiera afectado a un número indiscriminado de víctimas. Si el hecho se cometiere con el fin de obtener información sensible a la defensa nacional, el máximo de la pena de prisión se elevará a cuatro años.

“Capítulo 5 Disposiciones generales”

El artículo 503 establece que en alguno de los delitos previstos en el título en cuestión, hubiere intervenido un funcionario público, en ejercicio u ocasión de sus funciones, se le impondrá, además, pena de inhabilitación especial por el doble del tiempo de la condena a prisión.

Una buena opción es incorporar dentro de disposiciones generales el agravante de la pena para los casos donde interviene un funcionario público, en lugar de la redacción vigente, donde se incorpora al final de cada artículo una pena distinta.

Finalmente insisto en que ciertas cuestiones se han escapado de la órbita del proyecto; así se omiten alguna de las **conductas contenidas en el primer capítulo**, las que fueron objeto de mi análisis, vrg. Sextorsion, Spyware, los deepfake. Por otro lado otras como el Revenge porn o la suplantación de identidad fueron tratadas.

Este aspecto tiene que legislarse dentro de los delitos informáticos pero contemplando la ciberdelincuencia, es decir la organización criminal que utiliza este medio para potenciar sus conductas y valerse de los medios informáticos para su impunidad. (52/19, 2019)

Desde una óptica Internacional:

EL CONVENIO DE BUDAPEST

El Convenio Internacional de Budapest o “sobre Cibercriminalidad” tiene el papel protagonista junto al anteproyecto del Código Penal, dentro de este trabajo.

El mencionado Convenio fue aprobado por el Consejo de Europa, entró en vigencia en el 2004 y se ha incorporado a nuestra legislación mediante la ley 27.411, en el año 2017.

Dentro del preámbulo del Convenio se debe destacar que consideraron a dichas disposiciones como necesarias para prevenir actos que pongan en peligro la confidencialidad, integridad y disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, garantizando la tipificación como delito de dichos actos. También estimaron que la lucha contra la ciberdelincuencia requiere una cooperación internacional reforzada, rápida y eficaz en materia penal.

Sin lugar a dudas los redactores han logrado el objetivo, al haber escrito una norma que se haya mantenido con el paso de los años sin la necesidad de una constante reforma, por el conocimiento suficiente sobre el tema y la capacidad de prever nuevas conductas.

Antes de analizar el Convenio debo cuestionar un aspecto del mismo y es que hay conductas disvaliosas que no contempla; pero en cambio el anteproyecto del Código Penal si lo hace; entonces si este último estuviera sancionado en la actualidad, implicaría un gran avance sobre la delincuencia informática.

Como mencione respecto a la Ley 26.388 se utiliza la misma metodología, definir desde un comienzo los términos más relevantes. Claro que en determinadas leyes esto es algo común, pero no es la regla y además la comparación es válida porque se trata de disposiciones similares.

En primer lugar determina que un sistema informático será aquel dispositivo cuya función sea el tratamiento automatizado de datos en ejecución de un programa. Por dato informático se entenderá la representación de hechos, información o conceptos que

se preste a tratamiento informático, incluidos los programas empleados para que un sistema informático ejecute funciones.

Al definir proveedor de servicios se realiza una distinción, en primer lugar que será toda entidad que ofrezca a los usuarios de sus servicios la posibilidad de comunicarse por medio de un sistema informático y además cualquier entidad que procese o almacene datos de las mismas características.

Medidas que deben adoptarse:

Bajo este título se imponen algunos deberes para los Estados signatarios, los mismos consisten en una modificación de sus normas penales con el fin de establecer la tipicidad de determinadas conductas, a saber:

El *acceso ilícito*: Consiste en el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Para que el tipo se configure se deja a consideración de cada Estado que se puede hacer la siguiente elección: Exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informático u otra intención delictiva o bien el relación con un sistema informático conectado a otro.

La *interceptación Ilícita*: Será aquella conducta que de forma deliberada e ilegítima pretenda interceptar datos informáticos en transmisiones no publicas dirigidas a un sistema informático, originadas en el o efectuadas dentro del mismo. También faculta a los signatarios a tipificar que el delito se cometa con intención delictiva o en relación a un sistema informático conectado a otro.

Sobre la integridad de los datos, los mismos deben ser legislados en cuanto todo acto deliberado e ilegítimo dañe, deteriore, elimine o altere datos informáticos. Se faculta a los Estados a exigir que los actos comporten “daños graves”.

Respecto a la integridad del sistema se señala que importará la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático, introduciendo, alterando o transmitiendo datos informáticos.

Algo adelantado en ese entonces fue regular el abuso de los dispositivos:

Así se determinó que las siguientes conductas debían ser tipificadas:

Producción, venta, importación, utilización, difusión de cualquier dispositivo, incluido programa informático, concebido o adaptado para la comisión de los delitos mencionados anteriormente ; de una contraseña, Código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático. La posesión de

algún elemento como contraseña o Códigos de acceso para cometer algunas de las conductas mencionadas anteriormente. Exime de responsabilidad penal a quien posea alguno de los medios mencionados en tanto no tenga por objeto cometer los delitos mencionados.

También se expide sobre la falsificación informática; el fraude informático: como el destinado a causar un perjuicio patrimonial mediante manipulaciones de datos informáticos o interferencia en su funcionamiento; con la intención de obtener de forma ilegítima un beneficio económico.

La Convención en ese entonces también tuvo una eficacia plena, cuando se refirió a la obligación de tipificar los delitos relacionados con la pornografía infantil. Esto es algo sumamente admirable y que coloco en alza ya que fue lo suficientemente lucida como para prever que estas conductas se realizarían también por estos medios; los del internet.

Sobre estos delitos los tipos penales son los que hoy en día están en nuestra legislación, con la salvedad de que la Convención por ese entonces, en su artículo 9 inciso d, se refirió a la “adquisición para uno mismo o para otros de pornografía infantil” y en su inciso e “la posesión de pornografía infantil”; algo incorporado en el año 2018 en nuestra legislación; como bien mencione anteriormente. A esto me refiero cuando expreso que la convención fue lo suficientemente lucida, fue tan acertada que se adelantó a determinadas controversias; ese tipo penal ausente hasta hace no tanto fue previsto hace más de catorce años.

Si bien la Convención en la actualidad debería ser pasible de una modificación, la considero autosuficiente al punto de haber tenido éxito en regular estos aspectos durante tanto tiempo.

En su título cuarto se refiere a los delitos relacionados con infracciones a la propiedad intelectual. Por mi parte seguiré la misma metodología que el anteproyecto del Código Penal; para mí son pasibles de un título a parte, por lo que no están comprendidos dentro del objeto de mi trabajo final. De todas formas considero excelente que se haya previsto también este aspecto en la Convención.

Bajo otro título la Convención trata el derecho procesal; por ser derecho de forma no será parte del análisis de este trabajo.

Lo que sí me parece destacable es la “Obtención en tiempo real de datos informáticos”, aquí se trata de reglar que los Estados parte faculden a sus autoridades

competentes para: Obtener u obligar a proveedores de servicios a obtener o grabar u ofrecer a las autoridades su colaboración y asistencia para obtener o grabar en tiempo real datos relativos al trafico asociado a las comunicaciones transmitidas por medio de un sistema informático dentro de ese territorio. Esta norma la encuentro favorable porque es la mejor expresión del pilar fundamental:” “La tecnología como herramienta de prevención” y esto nada tiene que ver con la responsabilidad limitada que tienen las ISP sino el compromiso que deben tener con las autoridades para esclarecer determinadas situaciones o investigaciones sobre determinados hechos.

Sobre la Cooperación Internacional también se pronuncia; esto es algo lógico ya que es una clave para la detención de estos delitos. Establece así determinados principios generales, enunciando que las parte cooperaran entre sí en la mayor medida posible, con la aplicación de instrumentos pertinentes sobre cooperación internacional en materia penal a efectos de las investigaciones relativas a los delitos descritos para obtener prueba en formato electrónico. Entre lo considerado como más relevante destaco:

1. Se aplica la extradición entre las partes por los delitos mencionados siempre que sean castigados o penados la legislación de las dos partes implicadas en el hecho y con una pena privativa de la libertad de duración de al menos un año o con una pena más grave. Es decir que si la pena es menor a un año no correspondería la extradición. De allí la importancia de la pena proporcional al hecho cometido para luchar contra la delincuencia organizada en materia de delitos informáticos.

2. Cuando se aplique una pena mínima diferente en virtud de un tratado de extradición aplicable entre dos o más partes, incluido el Convenio Europeo de Extradición o de un acuerdo basado en la legislación uniforme, se aplicara la pena mínima prevista.

En el artículo 25 se establecen principios sobre la asistencia mutua, a efectos de las investigaciones o procedimientos relativos a estos delitos y datos informáticos para así obtener prueba electrónica, también faculta a las partes a formular una solicitud de asistencia mutua o realizar comunicaciones relativas a la misma a través de medios de comunicación rápidos siempre que el medio empleado sea seguro y eficaz.

Si todos los elogios que el Convenio ha recibido no son suficientes debo mencionar la “Red 24/7”. Es un sistema por el cual cada parte debe designar un punto de contacto localizable las 24 hs del día, siete días de la semana, para garantizar una

asistencia inmediata para investigaciones relativas a estos delitos o para obtener pruebas en formato electrónico. (Convenio sobre cibercriminación del consejo de Europa, 2017)

Respecto a las reservas:

1- Tipificación de actos preparatorios

La primera reserva está vinculada con lo que se denomina actos preparatorios, la reserva es sobre el artículo 6 del Convenio, específicamente el inciso b; por lo que respecto al abuso de dispositivos no se tipificara la tenencia de Códigos de acceso, contraseñas, etc.

2- Figuras incompatibles con el Código Penal

La segunda reserva se refiere a los arts. 9.1 “d” y 9.2 “b” y “c”. En este caso, el legislador funda la reserva en que dichas normas se referirían a figuras penales incompatibles con nuestro Código Penal.

La adquisición para uno mismo o para otros de pornografía infantil a través de un sistema informático. (Se interpreta que con la reforma introducida por la ley 27.436 esto quedaría sin efecto, al estar tipificada la mera tenencia de este material) - Una persona que parezca un menor adoptando un comportamiento sexualmente explícito- Imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito. – Estas situaciones no están previstas actualmente en la legislación penal.

3- Reserva parcial respecto de la tenencia de pornografía infantil

La tercera reserva se refiere al art. 9.1.e, que compromete a tipificar la “posesión de pornografía infantil”. Hoy esto ha cambiado por medio de la ley 27.436 como se menciona, ya que la tenencia de pornografía infantil está penada.

4- Incompatibilidad con las reglas de competencia penal

La cuarta reserva es con relación al art. 22.d, que establece que cada Estado adoptara las medidas necesarias para afirmar su jurisdicción respecto de cualquier delito que se cometa en su territorio, ahora bien, la reserva que hace la Argentina es en el caso de que el delito se haya cometido por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en que se cometió o si ningún estado tiene competencia respecto del mismo.

5- Necesidad de doble incriminación para cooperación internacional

El art. 29 del Convenio de Budapest regula un procedimiento cautelar que permite la conservación rápida de datos informáticos almacenados. Este procedimiento versa en la cooperación internacional y tiene por finalidad que un Estado pueda requerir colaboración a otro en el marco de una investigación penal.

La República Argentina formuló una reserva al art. 29.4, por lo que puede negarse a una solicitud de asistencia mutua con vistas al registro o acceso, o bien relevación de datos informáticos cuando el Estado requirente no cumpla con la doble incriminación. Esto implica la condición de que en ambos Estados la conducta debe estar tipificada, tanto en el Estado requirente como en el requerido. Por lo que si Argentina recibe una solicitud de asistencia bajo este marco convencional y en el territorio eso no constituye un delito, Argentina podrá negarse a presar cooperación pasiva.

Sobre las disposiciones contenidas en el Convenio de Budapest Argentina cumple casi todas las mencionadas. La legislación penal fue fruto de ciertas modificaciones recientes las cuales aún y pese a cumplir gran parte de lo pactado en el Convenio; no replican la situación actual por hacer omisión de ciertas conductas informáticas.

Lo cierto es que el compromiso no debe ser solamente con la Convención sino también con todos los ciudadanos Argentinos, para procurar que sus derechos no se vuelvan letra muerta ante el avance de la tecnología.

Resolución 234/2016

En Bs. As., con fecha 07/06/2016 se crea la red 24/7, la misma que contempla el Convenio de Budapest.

Dentro de los motivos que dieron origen a esta resolución se encuentran:

1. Que el incremento de los delitos cometidos a través de las nuevas Tecnologías de la Información y Comunicaciones (TICs) en la última década deviene en una necesidad de capacitar y dotar a las Fuerzas de Seguridad y Policiales con herramientas, métodos y procedimientos a fin de mejorar su investigación y conservar la prueba digital.

2. Que los delitos informáticos o ciberdelitos son actividades delictivas en donde las TICs se utilizan como medio para la comisión o bien, son objetos del delito

(acceso ilegítimo a sistemas o datos restringidos, daño informático, denegación de servicios, etc.).

3. Que el anonimato que provee la utilización de Internet y las redes sociales dificulta la persecución de los delitos cibernéticos

4. Que la prueba digital se diferencia de la prueba tradicional por su volatilidad, la capacidad de duplicación de la misma, la facilidad para alterarla y la cantidad de meta-datos que posee.

Así se aprobó el protocolo general de actuación para las fuerzas policiales y de seguridad en la investigación y proceso de recolección de pruebas en Ciberdelitos. En el anexo se explican entre otras cosas las reglas de actuación, como así también se brindan definiciones: como:

- Ciberdelito: “todo delito en donde las Tecnologías de la Información y las Comunicaciones (TICs) sean utilizadas como medio para la comisión del mismo o bien sean el objeto.

- Grooming: delito que se configura cuando por medio de comunicaciones electrónicas, se contacta a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.”
Copia Forense: réplica en forma completa de la estructura y contenido de un dispositivo de almacenamiento.

- Evidencia digital: es la prueba fundamental en los ciberdelitos. Información y datos de valor en una investigación que se encuentra almacenada, es recibida o transmitida por un dispositivo electrónico. Normalmente las pruebas consisten en archivos digitales de texto, vídeo o imagen, que se localizan en ordenadores y todo tipo de dispositivos electrónicos.

Contempla también los bienes objeto de eventuales secuestros:

- Computadoras: Gabinetes, motherboards, microprocesadores, discos rígidos, tarjetas de memoria, laptops, baterías.

- Dispositivos periféricos: Hardware que puede ser conectado a una computadora para mejorar y expandir las funciones de la máquina, estos en función del ADN que pueda recolectarse).

- CD, DVD, Pendrives, Tarjetas de memoria. Celulares, smartphones, tablets, También cualquier otro tipo de dispositivo que pueda contener: Documentos, imágenes, fotos, email, historial de navegación, log de los chats, discos externos, geo-localización.
- Respecto a esta resolución al ingresarse a las direcciones de internet del gobierno se podía observar que esto estaba orientado al ámbito de prevención de pornografía infantil. (Resolución 234/16, 2016)

Resolución 1291/19

A fines del 2019 se creó mediante el ministerio de justicia la unidad 24/7 de delitos informáticos y evidencia digital. La misma prestara asistencia en la investigación de estos delitos y en la recolección de la evidencia digital. Es ahora cuando finalmente se dará cumplimiento al compromiso asumido en el 2017 al ratificar el Convenio de Budapest. Así la unidad creada actuara en forma coordinada con cancillería y será el órgano central de cooperación internacional. Todo esto bajo el artículo 35 de dicho convenio, donde se establecía la creación de un punto de contacto que opere de forma localizable, las 24 hs. del día, los 7 días de la semana, prestando asistencia inmediata para la investigación de dichos delitos. (24/7, 2019)

Resolución 977/19

Por medio de esta resolución se aprueba el plan federal de prevención de los delitos informáticos y la estrategia de seguridad cuya finalidad es brindar “un contexto seguro para el aprovechamiento del Ciberespacio por parte de los ciudadanos y organizaciones públicas y privadas, desarrollando de forma coherente y estructurada, acciones de prevención, detección, respuesta y recuperación frente a las ciberamenazas, conjuntamente con el desarrollo de un marco normativo acorde.”

La resolución mencionada debe ser traída a colación porque expresa la preocupación del sector Estatal sobre la problemática que estoy tratando. Lo que debe tenerse en cuenta es que la normativa no alcanza a la realidad y se requiere con urgencia una modificación en la ley penal. (977/19, 2019).

Cierre de capítulo.

Como cierre del mismo y contemplando todo lo mencionado me resulta necesario destacar, nuevamente, la importancia del proyecto del Código Penal y queda manifiesta la necesidad de que se sancione finalmente el mismo, con las salvedades que introduce.

Por lo tanto pese a tener normativa sobre el tema, hay cuestiones que no están aún tipificadas y deben ser relevantes para el legislador por las vulneraciones causadas en los ciudadanos. Así la norma debe regular todos los aspectos que han surgido motivo de las nuevas tecnologías. El proyecto del Código Penal es el más adecuado al Convenio de Budapest y el más indicado para cumplir todos sus aspectos ya que deja de lado la “urgencia por cumplir” un Convenio y se preocupa realmente por tomar cartas en el asunto.

Así Palazzi sostuvo que: La ley 26.388 no introdujo una reforma omnicompreensiva. No se legisló por ejemplo sobre robo de identidad porque esa figura estaba cubierta en forma abarcativa por la estafa y la falsedad de documentos. Sin embargo queda más que claro que en materia de robo de identidad existe un enorme vacío de parte del Estado en prevención y educación de usuarios de Internet y una real toma de conciencia de entidades financieras. Tampoco se legisló sobre propiedad intelectual, dado que esta materia está regulada por nuevos tratados internacionales. Finalmente la cuestión probatoria no fue abordada porque la reforma apuntó solo a modificar el Código Penal. (Palazzi, 2016, pág. 24)

Capítulo 3 – “La vulneración de derechos constitucionales en la red”.

“El listado de los derechos constitucionales personalísimos comienza por el reconocimiento de ciertos derechos fundantes, básicos y necesarios para la realización de los demás.” Continúa Saguéz: *en ese orden de ideas, cabe incluir primero los derechos a la vida, a la integridad corporal y psíquica, a la salud y dignidad, al nombre, nacionalidad, honor y a la propia imagen.* Y por último añade que: *“Todos ellos atañen a algo indispensable: **“que al ser humano se le reconozca condición de tal.”*** (Saguéz, 2003, p. 317)

La cuestión planteada en el presente capítulo será sobre los derechos constitucionales afectados por la comisión de estas conductas disvaliosas informáticas que aún no han sido legisladas (conductas mencionadas en el Capítulo 1°) es de vital importancia. Toda vez que estos derechos constitucionales son el fundamento teórico del problema a tratar ya que los derechos que se ven vulnerados son de esa índole. Ahora bien, ¿es cuestión suficiente que un derecho reconocido por normas con jerarquía Constitucional y supralegal sea objeto de protección por la norma penal? Contextualizando el momento social en el que nos encontramos y contemplando además que el “Internet” atraviesa todas las esferas de nuestra vida, considero que sí, toda vez que las acciones de terceros avasallen los derechos de una o más personas.

Sostengo que hay conductas disvaliosas que apuntan a lesionar distintas orbitas de los derechos. Una es la afectación a la esfera patrimonial y otra muy distinta es la esfera extrapatrimonial. Ambas obtienen la protección en el Código Penal actual pero en distintos delitos. Encontramos la afectación a la vida, la libertad, la integridad sexual, la privacidad. Estas esferas pueden verse afectadas conjuntamente en un delito o bien de forma separada; así el bien jurídico que protege la vida se materializa en el actual artículo 79. Por otro lado la protección a la privacidad se materializa en los artículos 162 y ss. Una afectación de forma conjunta puede observarse al lesionar la vida y la propiedad, así el artículo 165 dispone que se imponga reclusión o prisión de diez a veinticinco años, si con motivo u ocasión del robo resultare un homicidio. Sobre los delitos informáticos específicamente la órbita de protección que brinda el ordenamiento jurídico está enfocada a la esfera patrimonial. Dicho esto debe contemplarse que en las situaciones no se contempladas por la norma, la esfera más vulnerada es la extrapatrimonial, específicamente donde se afecta la intimidad;

Puntualmente en esos casos considero que el legislador debe expedirse; tipificando así toda conducta disvaliosa informática que sea lesiva de la intimidad.

Los delitos contemplados amenazan distintos derechos personalísimos, los que han sido objeto de regulación por la norma penal, han sido aquellos amparados bajo el artículo 17 de la CN: “La propiedad es inviolable, y ningún habitante de la Nación puede ser privado de ella, sino en virtud de sentencia fundada en ley.” Por lo mencionado el bien jurídico protegido en un caso de Fraude informático, daño informático, entre otros, es la propiedad. A fin de cuentas es lo que se afecta al incurrir en la conducta tipificada.

Ahora bien, sobre el derecho a la intimidad la cuestión se torna un tanto compleja. Se creería que con la sanción de la Ley 26.388 la misma está cubierta en todas sus matices, pero he demostrado que no es así, el mejor ejemplo son las conductas mencionadas que no tienen el amparo de la norma legal, que afectan el derecho a la intimidad específicamente y que son omitidas por el legislador.

En el comienzo de este trabajo sostuve que no soy partidaria de un positivismo extremo, que la norma no puede contemplar todos los supuestos porque los mismos son infinitos; que lo que se debe lograr es una norma capaz de adaptarse a distintas situaciones. Y en particular con este tipo de delitos lo que se debe aspirar es a la redacción y posterior sanción de una norma capaz de perdurar en el tiempo, sin volverse arcaica. La ventaja en legislar de esta forma es que el legislador no debe modificar la norma constantemente, que la norma se puede adaptar a la realidad social, acompañando la misma y siendo útil para la sociedad. A fin de cuentas las normas deben tener una utilidad, por eso son sancionadas.

Por lo tanto debe haber un marco jurídico en donde encuadrar distintas situaciones o hechos. En la actualidad este “marco” no existe, el primer proyecto de Código Penal capaz de “comprender” esta problemática es el que he analizado. Entonces hasta que este no sea sancionado los particulares estarán expuestos por las situaciones que la norma actual no contempla.

Como bien mencione, la protección a otorgada, al derecho de la privacidad, por la ley 26.388 es un tanto deficiente por no comprender totalmente la distinción entre privacidad e intimidad. Si bien se incorpora la privacidad como un bien jurídico protegido entiendo que es bastante limitado el alcance otorgado por el legislador en las figuras que ha introducido en la mencionada ley.

Así Horacio Nager advierte: Con respecto al término escogido en la Ley N° 26.388, lo privado puede no ser íntimo, de manera que el legislador, optó por la fórmula

más amplia a la hora de receptar posibles actos lesivos al núcleo ético social protegido. Esta elección terminológica se encuentra posiblemente inspirada en el derecho anglosajón donde se ha definido a la privacidad como el derecho a estar libre de injerencias indebidas o arbitrarias, sea que éstas provengan de terceros o del Estado. (Nager, 2011)

Dicho esto se observa que actualmente hay una desprotección de determinados bienes jurídicos, lo que implica una vulneración en los derechos consagrados en la Carta Magna.

Entonces retomando el punto de los derechos afectados, ¿Cuáles son estos derechos constitucionales que estas conductas vulneran? El derecho a la intimidad es el primero, también podría analizarse el derecho al honor, a la imagen, entre otros; pero el más significativo es el de la intimidad. En otras conductas mencionadas la propiedad también se ve afectada pero la misma tiene una importancia que data de hace varios años; siendo que lo que más se ha descuidado es el derecho a la intimidad.

En base a lo mencionado analizare la importancia del derecho a la intimidad, el derecho que ha sido más vulnerado en los últimos años.

Análisis del derecho a la intimidad.

Dice Eduardo Molina Quiroga remontándose a los antecedentes de esta protección, que hay que remitirse al SXIX, ya que hasta ese entonces era considerado como un bien del denominado “respeto moral debido a la persona”; esto último citando a Frossini Vittorio y otros.

Luego citando a Fernandez Sessarego, plasma que el Alemania específicamente en 1880, Kohler se refirió a un derecho individual que protege el secreto de la vida íntima de la publicidad no autorizada. Ya en un punto de acuerdo en común, distintos autores citan un trabajo que marcó un antes y un después en el análisis de este derecho. (Molina Quiroga, 2013, p. 3 y ss.)

En the Harvard Law Review el 15 de Diciembre de 1890, Samuel D. Warren y Louis D. Brandeis publicaron un trabajo, en él se contempla como se deben comprender y analizar ciertos derechos. La primera referencia al “derecho de dejarse en paz” o “right to be let alone” guarda relación con los dichos del Juez Cooley.

De forma instantánea el derecho a la intimidad aparece entrelazado con “las fotografías instantáneas” y como la prensa ha invadido los recintos sagrados de la vida privada y doméstica. En ese artículo se hace referencia a la invasión por parte de la prensa y se ejemplifica (a tono con la temática abordada) que los detalles de las

relaciones sexuales se difundían en las columnas de los periódicos, todo esto promovido por el comercio lo que provocó que el individuo se haya sentido sensible ante estas injerencias y la privacidad se ha vuelto esencial. (Brandeis & Warren, 1890, págs. 193-196).

Resulta curioso que en ese entonces la intimidad ya era afectada por parte del periodismo lo que volvía a los sujetos bastante sensibles, en las palabras de los autores. Hoy en día con el Internet todos estamos expuestos en un nivel mayor. Respecto a distintas opiniones acerca de la “exposición” en las redes sociales debo decir que independientemente de lo que una persona decida compartir en ellas sus derechos no pueden verse afectados por terceros. En otras palabras, el uso de internet y la publicación de contenido en el mismo no pueden servir de argumento para justificar la violación de ciertos derechos como lo es el derecho a la privacidad, el honor, la imagen.

En esta misma línea de pensamiento Palazzi sostiene que: *“Hoy en día es difícil argumentar el derecho a la privacidad en forma absoluta frente a tantos actos propios de los usuarios, pero esto no quiere decir que los mismos hayan renunciado a su vida privada”*. (Palazzi, 2019, p. 62)

Imaginemos que si en ese entonces la privacidad era frecuentemente vulnerada por la prensa, actualmente esto se ve potenciado por las redes sociales y no solo por parte del actuar de la prensa en las mismas sino de un sinnúmero de personas inimaginables. Claro que los usuarios de las redes cuentan con algunas herramientas para “intentar” preservar su intimidad. Así pueden utilizar perfiles privados y restringir sus publicaciones en Internet a la mera vista de sus “contactos”.

Lo cierto y preocupante es que en los delitos informáticos esas protecciones no tienen ningún valor. La persona que decide actuar de forma lesiva para los derechos de terceros tiene en cuenta las herramientas que Internet le brinda y las utiliza a su favor. Se llegó a un punto donde el derecho a la intimidad es claramente vulnerado pese a todas las precauciones que los sujetos puedan tomar, las injerencias en la vida privada son máximas.

Retomando la idea de Molina Quiroga, él mismo sostiene que el desarrollo del concepto de Derecho a la intimidad y la vida privada visto desde un marco ideológicamente liberal se presenta como el derecho a la libertad, por el cual el sujeto puede hacer lo que le parece, es decir, a estar en soledad, no ser incomodado, sus decisiones sobre su vida sexual, la “libertad a la identidad”. Todo esto se desarrolló a

fines del siglo XVIII. Introduce él mismo que la libertad puede tener una concepción en el sentido negativo, lo que implica no sufrir interferencias de otros. (Molina Quiroga, 2013, p. 4 y ss)

En este aspecto de la libertad en sentido negativo es que se desarrollarán ciertas conductas que deben ser pasibles de tipificación.

Quiero destacar algo que no puede pasar inadvertido, algo que debe servir como una suerte de “faro”.

Citando al Dr. Palazzi él mismo advierte que: *En 1976 el civilista, Guillermo Borda, propuso sancionar penalmente las violaciones a la privacidad por considerar que el Derecho civil no era suficiente para frenar los ataques en la vida privada.* Cuenta el autor que el Dr. Borda se refería a los ataques de la prensa amarilla y los fotógrafos. (Palazzi, 2019, p. 63)

Lo que no pudo prever es que en la actualidad la intimidad fuera a estar tan amenazada. Resulta increíble a mi parecer que este problema se haya planteado hace tantos años y que aún la ley no haya logrado responder de forma correcta ante tantas injerencias sobre un derecho tan valorado.

Contemplando entonces distintos análisis sobre el mismo derecho, otro autor como Horacio F Delpech se expide sobre el mismo tema. Contempla así que las nuevas tecnologías han traído problemas tales como afectar la intimidad de los individuos.

Así define al derecho a la intimidad como un derecho personalísimo que tienen los sujetos de excluir a terceros de su vida personal, atento a esto se contemplan los sentimientos, comportamientos y es lo que les permite determinar cómo y en qué medida las informaciones que les atañen puedan ser comunicadas a otras personas. (Fernández Delpech, 2016, p. 327)

El mismo autor sostiene que este derecho en cuestión se encuentra en pugna con el derecho a la información, ya que la intimidad implica resistirse al suministro de datos personales cuando sus requerimientos parecen abusivos y el derecho a la información trata de “lograrlos”.

Bajo este análisis el autor considera que cuando la intimidad “choque” es decir, este en pugna con el derecho a la información, el que debe ser protegido es el derecho a la intimidad. (Fernández Delpech, 2016, p. 329)

Palazzi considera que el derecho penal debe adaptarse a estas nuevas realidades y lograr respuestas acordes a la índole del derecho fundamental que se busca amparar. En una de sus notas sostiene que lo paradójico hoy en día es que si alguien tiene la

intención de esconder algo “íntimo” sería más seguro guardarlo en un lugar físico antes que en un ordenador o teléfono inteligente. (Palazzi, 2019, p. 62)

El origen Constitucional de este derecho en nuestro territorio emana del artículo 19, sosteniendo el mismo que las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe.

Consideraciones jurisprudenciales sobre este derecho

Posición de la Corte Suprema de Justicia:

“El derecho al honor y a la intimidad se encuentra consagrado en los arts. 19 de la Constitución Nacional, 11 de la Convención Americana sobre Derechos Humanos y 17 del Pacto Internacional de Derechos Civiles y Políticos. En estos últimos se establece que toda persona tiene derecho a que se respete su honra y que nadie puede ser objeto de injerencias arbitrarias en su vida privada ni de ataques ilegales a su honor y reputación.

Por su parte, el derecho a la imagen integra el derecho a la privacidad protegido por el artículo 19 de la Constitución Nacional. Al respecto, esta Corte ha dejado claramente establecido que dicha norma otorga al individuo un ámbito de libertad en el cual éste puede adoptar libremente las decisiones fundamentales acerca de su persona, sin interferencia alguna por parte del Estado o de los particulares, en tanto dichas decisiones no violen derechos de terceros. Así, en Fallos: 306: 1892 el Tribunal estableció que el citado artículo 19 "...protege jurídicamente un **ámbito de autonomía individual constituida por los sentimientos, .hábitos y costumbres**, las relaciones familiares, la situación económica, las creencias religiosas, **la salud mental y física** y, en suma, las acciones, hechos o datos que, teniendo **en cuenta las formas de vida aceptadas por la comunidad están reservadas al propio individuo y cuyo conocimiento y divulgación por los extraños significa un peligro real o potencial para la intimidad**. En rigor, el derecho a la privacidad comprende no sólo la esfera doméstica, el círculo familiar y de amistad, sino a otros aspectos de la personalidad espiritual o física de las personas tales como **la integridad corporal o la imagen** y nadie puede inmiscuirse en la vida privada de una persona ni violar áreas de su

actividad no destinadas a ser difundidas, sin su consentimiento o el de sus familiares autorizados para ello y sólo por ley podrá justificarse la intromisión, siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen ..." (en igual sentido, Fallos: 335:799).” (Rodríguez c/ Google inc. s/ Daños y perj., 2014)

De esta forma tal y como se observa la CSJN sigue el criterio por el cual se determina que el derecho a la privacidad contiene el derecho a la intimidad y este a su vez comprende la dignidad, el honor y la imagen de las personas. Resulta necesario comprender que en la afectación de estos derechos por la comisión de las conductas mencionadas a lo largo de este trabajo final, solo el Estado es capaz de intervenir y tomar la “batuta” para así detener estas vulneraciones. Cuando se actúa de esta forma disvaliosa no hay elementos efectivos para que el individuo detener estas conductas lesivas de derechos fundamentales.

Por otro lado se debe tener en cuenta que al promover legislación penal sobre estas conductas disvaliosas informáticas no solo se protegerá a eventuales víctimas sino también a los derechos de todos los usuarios de internet, ya que una consecuencia de la tipificación de las mismas será establecer la **responsabilidad para el autor o los autores de dicho actuar lesivo y no para los intermediarios.** Un asunto muy común en el acontecer de esas conductas es demandar a los proveedores de servicios de internet, los cuales son meros intermediarios y como se ha comentado y fundado en base a lo argumentado por la Corte suprema de Justicia, en el fallo citado, no tienen responsabilidad por el contenido de terceros. Por otro lado las demandas civiles contra los PSI o ISP, en inglés, disminuirán toda vez que se las intente responsabilizar por el contenido de terceros, con las excepciones ya mencionadas.

Ciclo de conferencias maestros del Derecho, vinculado con el trabajo final:

Dentro de este ciclo de conferencias me valdré del material brindado por el Dr. Profesor y Vicedecano de esta casa de estudios; el Sr. Alejandro J. Laje, donde en la presentación a su libro el derecho a la intimidad imparte un conocimiento sumamente valioso y relevante con tal problemática. La relación es visible e incuestionable, estas conductas disvaliosas que se han tratado a lo largo de este trabajo final encuentran su punto en común en cuanto en su mayoría se vulnera el derecho a la intimidad de la víctima; en otros casos se expande la órbita de derechos personalísimos vulnerados,

siendo los mismos el derecho a la libertad, a su honor, etc. Y con derecho a la libertad Me refiero **no** a la libertad física **en el estricto sentido de la palabra**, sino en un sentido de la autonomía de la voluntad para compartir o dar a conocer determinado contenido de carácter personal o íntimo, del afectado; el cual podría llegar a ser considerado una extensión del derecho a la libertad en esta nueva era digital.

Es por lo expuesto que pasaré a compartir distintas consideraciones para comprender el alcance del derecho a la intimidad. **Las mismas serán captadas y producidas de forma casi literal para poder transmitir la esencia y no distorsionar el valor de sus palabras y sus ideas, realizando la cita correspondiente.**

“No resulta fácil establecer los límites para su protección a pesar de que la legislación Nacional e internacional establece pautas para su limitación. Resulta que la libertad de intimidad legítimamente encuentra restricciones con los requisitos de la vida democrática, la investigación del crimen, los problemas de seguridad, entre otros, requieren que legítimamente haya intervenciones a la intimidad para planificar otros aspectos que hacen al interés general de la vida en sociedad.

Por tanto determinar el ámbito de su protección no resulta fácil tanto para la doctrina como para la jurisprudencia. Luego el Dr. Realiza una síntesis sobre la evolución de la intimidad. Se remite en primer lugar a los Griegos, los cuales no reparaban en el interés sobre la intimidad ya que la importancia para los mismos era la vida pública. Un hito importante lo remite a San Agustín, él decía que “no había que buscar fuera del hombre lo que lo hacía pleno ya que en su interior encontraba lo más importante que era Dios mismo, allí el Occidente repara en las bases sobre este Derecho.

Los límites precisos se los atribuye al filósofo Immanuel Kant, considerando que todo ser racional debería ser considerado como un fin en sí mismo y jamás como un medio.

Aquí se imponen los límites de la dignidad humana que requieren de la autodeterminación al momento de ser considerados un fin en sí mismo y luego a partir de allí se centra la importancia del individuo y de la subjetividad del mismo; por otro lado esto es pasado en limpio a nuestra Carta Magna, en el artículo 19.

Según el citado autor, dos jueces norteamericanos establecieron las pautas modernas para la protección a la intimidad, estos jueces establecieron que existe un derecho de la persona a estar solo, a auto determinarse en las cuestiones fundamental de sus ideas, sentimientos y fundamentalmente en el modo en que quiero darlo a conocer.

Esto último marca la gran actualidad del derecho a la intimidad, el modo en el que queremos dar a conocer estas ideas pertenece al ámbito de la autodeterminación de las personas.” (Comprender el derecho, Conferencias de la Universidad Abierta Interamericana, 2014)

A partir de esta última consideración y exposición de la tan valiosa investigación realizada por el mencionado autor es que expongo lo que comprende el derecho a la intimidad, **la protección que se le debe otorgar por parte de la norma penal y por esto remarco la importancia que reviste la prevención de estos “Delitos informáticos” por considerarlos sumamente lesivos de la intimidad, dignidad y en algunos casos el honor, de la persona humana.**

Protección otorgada por Tratados internacionales.

1. DECLARACIÓN AMERICANA DE LOS DEBERES Y DERECHOS DEL HOMBRE.

Esta declaración fue aprobada en la Conferencia Internacional Americana IX, en 1948, específicamente en la ciudad de Bogotá, Colombia. Tiene como parte de su fundamento la idea de que la protección internacional de los derechos del hombre debe ser la “guía principalísima del derecho americano en evolución”.

Dentro de los derechos reconocidos, son destacados los siguientes:

El derecho que todo ser humano tiene a la vida, a la libertad y a la seguridad de su persona. Este texto forma parte del primer artículo de la Declaración y es fundamental por el derecho conferido a la libertad. Se debe recordar la relación que tiene con el derecho a la intimidad, como la esfera del derecho a la libertad negativa.

Por otro lado el artículo cuatro hace una referencia expresa a los derechos que toda persona tiene a opinar, expresarse y difundir su pensamiento por cualquier medio.

Así las interacciones o publicaciones en redes sociales, plataformas digitales o el Internet en su sentido más amplio, no puede ser objeto de restricciones de particulares ni del Estado en cuestión, a excepción de que se vulneren derechos reconocidos en una norma. Es decir la libertad para actuar en Internet es amplia pero la misma no puede afectar derechos de terceros o podrá verse limitada por la autoridad Estatal en cuestión. Hasta aquí no habría ninguna diferencia con la regulación que se aplica para el mundo “físico”.

El artículo cinco establece que toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar.

A mi entender es otro artículo que tiene un nexo directo con el tema de este trabajo. Los ataques que surgen de publicaciones o divulgaciones de ciertos materiales por el Internet deben tener una norma que establezca su protección y esta, entiendo que debe superar el mero resarcimiento económico, aquí se está en presencia de actos que requieren ser alcanzados y regulados por el Derecho Penal. Esto es así porque son situaciones un **poco** similares a las que suceden por la Violación de Secretos, injurias, pero destacando que el medio del Internet potencia sus efectos negativos, sirve de “escudo” para cubrir ciertos actos; lo cual es una creencia antigua ya que en el marco de una investigación puede determinarse y probarse adecuadamente cada “rastro digital”; es decir, todo queda registrado. Además el o los autores se valen de ese medio para, en muchas ocasiones, aprovecharse del anonimato que brinda ese medio; también es notorio que la lesión causada a determinado derecho verá su expansión territorial sin fronteras, es decir no habrá un límite donde se detenga, el hecho provocado será transnacional en la mayoría de los casos. De más está decir que la figura de Violación de secretos o injurias no puede aplicarse por no estar permitida la analogía, de todas formas esto ya ha sido desarrollado.

Del artículo dieciocho se desprende textualmente que toda persona puede concurrir a los tribunales para hacer valer sus derechos. Este derecho conocido como acceso a la justicia será posible toda vez que una norma faculte al sujeto a recurrir ante ella, en estas conductas planteadas observamos que la norma no los comprende, por lo que no hay acceso a la justicia en estos casos particularmente mencionados.

En el artículo veintiocho se establece que los derechos de cada hombre están limitados por los derechos de los demás, por la seguridad de todos y por las justas exigencias del bienestar general y del desenvolvimiento democrático. Esta disposición deriva en la expresión “sus derechos terminan donde empiezan los míos” y tiene injerencia en el presente trabajo porque cada acto que se ejerza en internet (y no solo en este) debe tener esta limitación, la libertad no puede ser absoluta ya que en el mundo “terrenal” tampoco lo es. De todas formas no puede derivarse en lo que es la censura por el solo hecho del derecho a la libertad de expresión. Pero toda vez que un acto cometido por una o más personas en internet y que se adecue a lo planteado a lo largo de los capítulos pasados; debe tener una sanción penal. (Declaración americana de los deberes y derechos , 1948)

2. DECLARACIÓN UNIVERSAL DE LOS DERECHOS HUMANOS.

En el año 1948 Argentina la proclama por la Resolución 217 de la Asamblea General de las Naciones Unidas.

Art. 1 Todos los seres humanos nacen libres e iguales en dignidad y derechos y, dotados como están de razón y conciencia, deben comportarse fraternalmente los unos con los otros.

Art. 12 Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Este artículo es el más trascendental desde el punto de vista del tema abordado, es la expresión más clara de la idea de este trabajo, la ley debe servir para la protección de derechos fundamentales sobre todo en los aspectos que al verse quebrantados pueden vulnerar enteramente a un ser humano.

Art. 19 Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.

Esta norma debe tenerse en cuenta ya que al intentar dar una respuesta desde la óptica civil, a esta problemática, solicitando por ejemplo medidas cautelares, deben tener en cuenta que la responsabilidad por dichos o derivados de los mismos es “ulterior” y esto obedece a evitar la censura previa. (Asamblea general ONU, 1948).

3. CONVENCIÓN AMERICANA SOBRE DERECHOS HUMANOS- PACTO DE SAN JOSÉ DE COSTA RICA

Suscripta en la ciudad San José de Costa Rica, Costa Rica, el 22/11/1969.

En su artículo cinco contempla el derecho a la integridad personal, así establece que:

1. Toda persona tiene derecho a que se respete su integridad física, psíquica y moral.

Esta integridad puede verse vulnerada en los últimos dos aspectos mencionados en el caso de la difusión de material sensible sin su consentimiento, la obtención del mismo tipo de material sin el conocimiento de la parte afectada o cualquier otro tipo de violación a la intimidad que ha sido mencionada anteriormente. Como se ha expuesto

anteriormente la jurisprudencia emanada de la Corte Suprema de Justicia de la Nación ha entendido que forma parte del derecho a la intimidad de una persona lo respectivo a su imagen, integridad y honor.

Art. 11. Protección de la honra y de la dignidad

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.

2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

Art. 13. Libertad de pensamiento y de expresión

1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente por escrito o en forma impresa o artística o cualquier otro procedimiento de su elección.

2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley....

Como bien mencione en lo respectivo a la Declaración Universal de los derechos humanos, en el comentario del artículo 19, la responsabilidad es ulterior para el que mediante internet genere, verbigracia, un daño a la reputación de una persona. Así la norma penal no impedirá que estos actos se cometan sino que penará al que cometa las conductas que regule. Lo que evitará que estas conductas proliferen será la combinación de los cuatro pilares fundamentales, teoría explicada en el primer capítulo. (Ley 23.054, 1984).

La protección a la imagen

En virtud de lo mencionado en el título anterior dentro de lo que comprende la privacidad se encuentra el derecho a la propia imagen. Autores comprenden que esta protección puede verse desde distintos sentidos, así uno de los posibles es relacionar este derecho con la facultad de una persona de decidir resguardar su imagen en la intimidad. Esta es la postura de Néstor P. Sagués, a quien citaré para desarrollar la perspectiva constitucional de este derecho personalísimo.

Así él comprende que la imagen no debe ser difundida sin la autorización de la persona cuya intimidad está comprometida, esta es la doctrina de la Corte Suprema, en el fallo "Ponzetti de Balbín".

En dicho fallo la Corte analizó la publicación de una fotografía del doctor Balbín, cuando agonizaba en una clínica, y concluyó que se había violado su derecho a la privacidad.

Otra versión del derecho a la "imagen pública" refiere al honor de las personas. Dicho de otra manera: *ciertas expresiones pueden dañar la imagen o el concepto social que se tiene de una persona.*

Una tercera expresión del derecho a la propia imagen consiste en reconocer a cada persona la facultad de vestirse o arreglarse como le parezca, respetando naturalmente a los demás y a la moral pública. Lo importante es subrayar que el derecho a la propia imagen tiende a perfilarse como derecho constitucional. Desde esta perspectiva, tal derecho impide la reproducción no consentida de las fotos de una persona, especialmente si se han tomado en su ámbito doméstico, aunque también en lugares públicos, en particular con fines lucrativos. También veda la utilización de la voz o del nombre de una persona sin su autorización. (Saguéz, 2003, pp. 345-346)

Esta perspectiva arroja luz sobre las esferas de protección que componen a la intimidad. Lejos de ser un derecho abstracto y acotado se observa como entraña la parte fundamental de los sujetos, la vida privada. Es de carácter notorio que la protección que se le debe otorgar a tal derecho debe coincidir con la magnitud del mismo. En este sentido todos podemos asegurar que es un derecho fundamental que nos pertenece individualmente y no puede ser objeto de intrusiones ajenas a la propia voluntad.

María C de Cucco Alconada manifiesta que es un derecho de carácter personalísimo pero que se puede analizar desde dos sentidos, distinto a como lo propone Sagués; así lo conforma un aspecto negativo el cual comprende la facultad que tiene un sujeto para prohibirle a terceros la captación o divulgación de su imagen y por otro lado en su aspecto positivo, aprecia la facultad de reproducir, publicitar o comercializar la imagen, según el criterio personal. (de Cucco Alconada, 2018)

Protección al honor y reputación, sus alcances.

Este derecho también quedará comprendido y tendrá relación con la temática planteada, así la Corte Suprema de Justicia en el fallo citado anteriormente (Rodríguez c/ Google inc. s/ Daños y perj., 2014). La jueza Highton de Nolasco entendió que “el derecho al honor se refiere a la participación que tiene el individuo dentro de la

comunidad amparando a la persona frente a expresiones o mensajes que lo hagan desmerecedor en la consideración ajena al ir en su descrédito”

Otros autores citan el fallo Ponzetti a fin de exponer argumentos judiciales para sustentar aún más este derecho, así la Corte Suprema en "Ponzetti de Balbín" marca una tendencia sobre la interpretación de este derecho.

Por otro lado en el fallo "Campillay" se establece que el honor, la reputación proceden del art. 33 de la Constitución Nacional.: *“Las declaraciones, derechos y garantías que enumera la Constitución no serán entendidos como negación de otros derechos y garantías no enumerados; pero que nacen del principio de la soberanía del pueblo y de la forma republicana de gobierno.”*

Según la doctrina de la Corte en "Costa", el derecho al honor justifica la sanción penal cuando actos lesivos lo ataquen y surge la responsabilidad civil consecuente buena reputación de las personas y en se ha establecido una relación con el derecho constitucional a la integridad moral y con el de dignidad individual de los sujetos. (Sagüez, 2003, pp. 344-345)

La identidad digital

El derecho a la identidad de los particulares está siendo lazado con el ámbito digital, esto concuerda con lo planteado en la introducción, al referirme a como el Internet y las redes sociales han modificado la estructura social y provocado cambios en la forma de vida.

En los tiempos que corren los sujetos son inseparables de las nuevas tecnologías, así la forma de comunicarse ha ido cambiando, de la misma forma en la que la identidad del sujeto se construye en el Internet. En las redes sociales por ejemplo, se comparten varios aspectos de la vida privada y se van construyendo distintos perfiles, donde la reputación es la clave.

Con el tipo de conductas planteadas a lo largo de este trabajo, específicamente las que lesionan no solo la esfera patrimonial sino también la extrapatrimonial, la identidad adquirida o formada en Internet es gravemente ultrajada por actos de terceros y sin el consentimiento del afectado.

*Hay autores partidarios de sostener que “de a poco se está conformando un nuevo **derecho** a la identidad digital, esto es, a existir en Internet y a estar protegidos al igual que en el mundo real, lo que no es un detalle menor porque, como se explicará infra, la trascendencia que tiene nuestra **imagen** digital (y sus lesiones) se encuentra a nivel mundial.”* (Bura Peralta, 2019)

Capítulo 4- “Una mirada al Derecho comparado”.

Se observa con frecuencia la incorporación de la normativa correspondiente a distintos sistemas jurídicos, generalmente “ya está dada por hecho” en los trabajos finales. Sin embargo el fin de incluir normas de derecho extranjero, en el presente trabajo, obedece a exponer el adelanto normativo de países tales como Brasil, España y Estados Unidos. Como bien relate en un principio de este trabajo una de las motivaciones que me llevo a elegir el tema fue una conferencia entre dos juristas, uno argentino y otro mexicano, donde comparaban la legislación de sus respectivos países sobre los “delitos informáticos”. Luego a medida que distintos hechos fueron siendo públicos el interés se acrecentó.

Cuando comencé a estudiar este tema en profundidad me dedique a observar la “situación normativa” de distintos Estados, con el fin de determinar si había una tendencia a considerar como delitos a aquellas conductas disvaliosas cometidas por medios informáticos y que sean lesivas de la esfera extrapatrimonial del sujeto, como puede ser el daño a la privacidad, intimidad, honor, etc. La respuesta a esta altura es fácilmente deducible, efectivamente me encontré con una legislación más severa y tendiente a proteger la intimidad de los usuarios en el Internet.

Con el fin de hacer posible una comparación entre nuestras normas penales y las de otros ordenamientos transcribiré las mismas.

1. Brasil

Brasil tiene una situación particular, ya que no solo se mostrará su normativa penal sino también “el marco civil de internet”. La misma es conocida como la Constitución de Internet, ésta es bastante evolucionada debido a los alcances de su regulación. Si bien se establecen derechos y garantías y no cumple la función de ser una norma penal; transcribiré determinados artículos a fin de observar el avance de dicho país.

a. Marco civil de internet

La sección integrada por responsabilidad por Daños que Surgieran del Contenido Generado por terceros está integrada por diversos artículos. Lo pertinente será analizar la regulación tendiente a los “proveedores de servicio de internet” y

contemplar sus disposiciones para así visualizar como esta temática es tratada hace ya algunos años por nuestro país vecino.

Artículo 18. El proveedor de conexión a Internet no será responsabilizado civilmente por daños surgidos por contenido generado por terceros.

Artículo 19. Con el objetivo de asegurar la libertad de expresión e impedir la censura, el proveedor de aplicaciones de Internet solamente podrá ser responsabilizado por daños que surjan del contenido generado por terceros si, después de una orden judicial específica, no toma las previsiones para, en el ámbito de los límites técnicos de su servicio y dentro del plazo asignado, tornar indisponible el contenido especificado como infractor, exceptuando las disposiciones legales que se opongan.

1º La orden judicial de que trata este artículo deberá contener, bajo pena de nulidad, identificación clara y específica del contenido especificado como infractor, que permita la localización inequívoca del material.

2º La aplicación de lo dispuesto en este artículo para infracciones a derechos de autor y a derechos conexos depende de la previsión legal específica, que Marco Civil Brasileño de Internet 37 deberá respetar la libertad de expresión y las demás garantías previstas en el artículo 5 de la Constitución Federal.

3º Las causas judiciales que traten sobre el resarcimiento por daños surgidos de contenidos disponibles en Internet relacionados a la honra, la reputación y a derechos de personalidad, así como sobre la indisponibilidad de esos contenidos por proveedores de aplicaciones de Internet, podrán ser presentadas mediante los juzgados especiales.

4º El juez, incluso en el procedimiento previsto en el 3º, podrá anticipar, total o parcialmente, los efectos de la tutela pretendida en el pedido inicial, existiendo la prueba inequívoca del hecho y considerando el interés de la colectividad en la disponibilidad del contenido en Internet, estando presentes requisitos de verosimilitud de la alegación del autor y de temor fundado de daño irreparable o de difícil reparación.

Artículo 20. Siempre que tenga informaciones de contacto del usuario directamente responsable por el contenido al que se refiere el artículo 19, corresponderá al proveedor de aplicaciones de Internet comunicarle los motivos e informaciones relativos a la indisponibilidad de contenido, con informaciones que permitan la contradicción y amplia defensa en juicio, salvo expresa previsión legal o salvo expresa determinación judicial fundamentada en contra...

Artículo 21. El proveedor de aplicaciones de Internet que haga disponible contenido generado por terceros será responsabilizado subsidiariamente por la violación de la intimidad resultado de la divulgación, sin autorización de sus participantes, de

imágenes, de videos y de otros materiales que contengan escenas de desnudos o de actos sexuales de carácter privado cuando, posterior al recibimiento de la notificación por el participante o su representante legal, dejar de promover, de forma diligente, en el ámbito y en los límites técnicos de su servicio, la indisponibilidad de ese contenido. La notificación prevista en el artículo deberá contener, bajo pena de nulidad, elementos que permitan la identificación específica del material apuntado como violador de la intimidad del participante y la verificación de la legitimidad para presentación del pedido.

Artículo 22. La parte interesada podrá, con el propósito de formar conjunto probatorio en proceso judicial civil o penal, en carácter incidental o autónomo, requerir al juez que ordene al responsable por la guarda u otorgamiento de registros de conexión o de registros de acceso a aplicaciones de Internet. Sin perjuicio de los demás requisitos legales, el requerimiento deberá contener, bajo pena de inadmisibilidad:

I – fundados indicios del acontecimiento del ilícito;

II – justificación motivada de la utilidad de los registros solicitados para fines de investigación o instrucción probatoria; y

III – período al cual se refieren los registros.

Artículo 23. Cabe al juez tomar las providencias necesarias a la garantía del sigilo de las informaciones recibidas y a la preservación de la intimidad, de la vida privada, de la honra y de la imagen del usuario, pudiendo determinar secreto de justicia, inclusive en cuanto a los pedidos de custodia de registro

En lo particular observo una tendencia lógica y aceptable a no responsabilizar a los ISP por el contenido de terceros excepto se lo intima por medio de una orden judicial a tomar determinadas previsiones sobre determinado contenido.

Respecto al procedimiento encuentro bien que se determinen algunos recaudos para asegurar que la libertad de expresión no sea vulnerada bajo ningún aspecto. Lo novedoso es el artículo 21 donde se establece una responsabilidad subsidiaria para aquel ISP que ponga a disposición del público contenido íntimo de una persona cuando sin su consentimiento. En lo que respecta a los artículos siguientes encuentro la misma línea argumentativa que a modo de apreciación personal considero que son normas muy favorables para todos los usuarios del Internet por igual. (LEY N° 12.965).

b. CÓDIGO PENAL DE BRASIL.

Ya en lo que respecta a la comparación planteada, el Código Penal de Brasil introdujo una serie de modificaciones en sus normas. Las mismas tratan los aspectos mencionados en el trabajo y son admirables desde un punto de vista jurídico.

Así en los años 2012 y 2018 respectivamente, por medio de la Ley N ° 13.772 y 12.737, se incorporan disposiciones sobre la “Exposición de la intimidad sexual”.

Original - PORTUGUÉS

Invasão de dispositivo Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: (Incluído pela Lei nº 12.737, de 2012)

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (Incluído pela Lei nº 12.737, de 2012)

1. Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. (Incluído pela Lei nº 12.737, de 2012)

2. Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico. (Incluído pela Lei nº 12.737, de 2012)

3. Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: (Incluído pela Lei nº 12.737, de 2012) Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

4. Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

-Traducción-

La invasión de dispositivo informático. Art. 154-A. Hackear el dispositivo informático de otra persona, esté o no conectado a la red informática, por incumplimiento indebido del mecanismo de seguridad y con el fin de obtener, alterar o destruir datos o información sin la autorización expresa o tácita del titular del

dispositivo o la instalación de vulnerabilidades para obtener una ventaja ilegal. Pena - detención, de 3 (tres) meses a 1 (un) año, y multa.

- Párrafo 1. La misma penalidad se aplica a aquellos que producen, ofrecen, distribuyen, venden o transmiten un dispositivo o programa informático para permitir la conducta definida en este capítulo.

- 2 La pena aumenta de un sexto a un tercio si la invasión resulta en una pérdida económica.

- 3 Si el resultado de la invasión es obtener el contenido de las comunicaciones privadas electrónicas, secretos comerciales o industriales, información confidencial, tal como se define por la ley, o el dispositivo de control remoto no autorizado invadieron, la pena será de prisión, de seis (6) meses a dos (2) años, y una multa si la conducta no es un delito más grave.

- Párrafo 4. En la hipótesis del Párrafo 3, la multa se incrementa de uno a dos tercios si hay divulgación, comercialización o transmisión a terceros, en cualquier capacidad, de los datos o información obtenida. (...)

Estos artículos precedentes son parte de la protección de la propiedad, en su mayoría y comprende en distintos tipos una gama de conductas bastante amplias que apuntan de forma correcta a comprender la mayoría de los problemas vinculados con la cuestión. Destaco el fin del inciso primero, el cual pena al que ponga a disposición los medios informáticos para cometer las conductas penadas.

Art. 216-B. Produzir, fotografar, filmar ou registrar, por qualquer meio, conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado sem autorização dos participantes: (Incluído pela Lei nº 13.772, de 2018)

Pena - detenção, de 6 (seis) meses a 1 (um) ano, e multa.

Parágrafo único. Na mesma pena incorre quem realiza montagem em fotografia, vídeo, áudio ou qualquer outro registro com o fim de incluir pessoa em cena de nudez ou ato sexual ou libidinoso de caráter íntimo.

Traducción

Art. 216-B. Producir, fotografiar, filmar o grabar, por cualquier medio, contenido con una desnudez privada o íntima o un acto sexual sin el permiso de los participantes. Pena - detención, de 6 (seis) meses a 1 (un) año, y multa. La misma pena se aplica a aquellos que realizan **montajes en fotografía, video, audio o cualquier**

otro registro para incluir a una persona en una escena de desnudos íntimos o actos sexuales o libidinosos.

Ahora es cuando la incorporación de Derecho comparado adquiere el mayor sentido todavía, el segundo párrafo del artículo sancionado en el año 2018 incluye a los “deepfakes” (explicados en novedosas conductas susceptibles de ser tipificadas), dentro del ámbito de la protección a la intimidad. De todas formas en mi análisis esto lo ubicaría como una figura general y no solamente orientada a la protección de la intimidad de los sujetos ya que también pueden generarse distintos problemas por adjudicarle una imagen y/o video a un tercero.

Divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia (Incluído pela Lei nº 13.718, de 2018)

Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia. Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave.

Aumento de pena 1º A pena é aumentada de 1/3 (um terço) a 2/3 (dois terços) se o crime é praticado por agente que mantém ou tenha mantido relação íntima de afeto com a vítima ou com o fim de vingança ou humilhação.

Exclusão de ilicitude 2º Não há crime quando o agente pratica as condutas descritas no **caput** deste artigo em publicação de natureza jornalística, científica, cultural ou acadêmica com a adoção de recurso que impossibilite a identificação da vítima, ressalvada sua prévia autorização, caso seja maior de 18 (dezoito) anos.

Divulgación de la escena de violación o escena de violación vulnerable, escena de sexo o pornografía.

Art. 218-C. Ofrecer, intercambiar, poner a disposición, transmitir, vender o exhibir para la venta, distribuir, publicar o divulgar, por cualquier medio, incluso a través de comunicación masiva o sistema informático o telemático, fotografía, video u otro registro audiovisual que contenga la violación de una persona vulnerable o que la aprueba o induce a ella o, **sin el consentimiento de la víctima**, sexo, desnudos o escena de pornografía. Pena: prisión de 1 (uno) a 5 (cinco) años, si el hecho no constituye un delito más grave.

Aumento de Penalización

1 La pena aumenta de 1/3 (un tercio) a 2/3 (dos tercios) si el delito es cometido por un agente que mantiene o ha tenido una relación cercana de afecto con la víctima o con fines de venganza o humillación.

Exclusión de ilegalidad

2 No hay delito cuando el agente practica la conducta descrita en el encabezado de este artículo en una publicación periodística, científica, cultural o académica con la adopción de recaudos que hagan imposible identificar a la víctima, excepto su autorización previa, si es mayor de 18 años. (CÓDIGO PENAL DE BRASIL, 1940)

Considero que esto puede vincularse con la transmisión de ilícitos por medios informáticos. Pero me refiero a transmisión “en vivo” por redes sociales, donde se busca delinquir y humillar a la víctima haciendo espectador a un público que puede o no, tener la intención de verlo. Lo destacable es la variante de verbos que integran el tipo, se han concentrado de forma satisfactoria en proponer una redacción amplia en un sentido tecnológico y que facilitara que la norma no se vuelva rápidamente obsoleta, conforme plantee en capítulos anteriores.

2. España

a. CÓDIGO PENAL DE ESPAÑA.

El título VI referido a los **Delitos contra la libertad**, dispone:

Artículo 172 ter.

1. Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que acose a una **persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes** y, de este modo, altere gravemente el desarrollo de su vida cotidiana:

1.^a La vigile, la persiga o busque su cercanía física.

2.^a Establezca o intente **establecer contacto con ella a través de cualquier medio de comunicación**, o por medio de terceras personas.

3.^a **Mediante el uso indebido de sus datos personales**, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.

4.^a Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella.

Si se trata de una persona especialmente vulnerable por razón de su edad, enfermedad o situación, se impondrá la pena de prisión de seis meses a dos años.

2. Cuando el ofendido fuere alguna de las personas a las que se refiere el apartado 2 del artículo 173, se impondrá una pena de prisión de uno a dos años, o trabajos en beneficio de la comunidad de sesenta a ciento veinte días. En este caso no será necesaria la denuncia a que se refiere el apartado 4 de este artículo.

3. Las penas previstas en este artículo se impondrán sin perjuicio de las que pudieran corresponder a los delitos en que se hubieran concretado los actos de acoso.

4. Los hechos descritos en este artículo sólo serán perseguibles mediante denuncia de la persona agraviada o de su representante legal. (CÓDIGO PENAL DE ESPAÑA)

COMENTARIO y JURISPRUDENCIA:

Entiendo que el artículo tiende a proteger la privacidad y la libertad de las personas afectadas por actos de terceros, siendo los mismos no consentidos. Esta conducta ya fue desarrollada bajo la denominación de “Stalking” y es otra de las que no contempla nuestro ordenamiento. Encuentro favorable que el derecho se adapte a las nuevas realidades, al fin y al cabo su carácter es dinámico.

Respecto a este artículo tan llamativo, una autora y abogada Española llamada Miriam Guardiola Salmerón reflexiona:

Que el bien jurídico protegido por el artículo es la libertad de obrar “entendida como la capacidad de decidir libremente”; esto sostiene que emerge de una sentencia dictada en España por el delito de Stalking, en el Juzgado N° 3 de Tudela. En la sentencia mencionada se destaca que: “de acuerdo con la exposición de motivos de la ley, este nuevo delito está destinado a ofrecer respuesta a conductas de indudable gravedad que, en muchas ocasiones no pueden ser calificadas como coacciones o amenazas. Se trata entonces de los supuestos en los que sin llegar a producirse necesariamente el anuncio explícito o no de la intención de coartar la libertad de la víctima, se producen conductas reiteradas por medio de las cuales se menoscaba gravemente la libertad y sentimiento de seguridad de la víctima a la que se somete a persecuciones o vigilancias constantes, llamadas reiteradas u otros actos continuos de hostigamiento. Así dentro de la exposición de motivos se introduce en el

bien jurídico protegido la seguridad, comprendiendo el derecho al sosiego y la tranquilidad personal. (Diligencias urgentes- Jurisprudencia española, 2016)

Por otro lado sostiene que las conductas de Stalking, afectan al proceso de formación de la voluntad de la víctima en tanto que la sensación de temor e intranquilidad o angustia que produce el repetido acechamiento por parte del acosador, le lleva a cambiar sus hábitos, sus horarios, sus lugares de paso, sus número de teléfono, cuentas de correo electrónico e incluso de lugar de residencia y trabajo. (Guardiola Salmerón, 2016)

Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, del descubrimiento y revelación de secretos.

Artículo 197. 1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando:

a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o

b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima.

Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años.

7. Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, **revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.**

La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el **cónyuge o por persona** que esté o haya estado unida a él **por análoga relación de afectividad, aun sin convivencia**, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.

COMENTARIO SOBRE LA JURISPRUDENCIA:

Respecto este artículo ya hay jurisprudencia disponible en España. Así por medio de la sentencia 201/2018, se condena a un hombre por acceder a una página web de alojamiento de videos pornográficos donde crea un perfil de usuario para difundir material sensible, de mujeres y niñas.

En el mismo sitio publicaba imágenes de mujeres, sin el consentimiento de ellas y hasta exponía los usuarios de “Instagram” de las mismas. De la sentencia surge que el acusado utilizó imágenes de perfiles privados con la finalidad de atentar contra la intimidad de las víctimas. También obtuvo imágenes grabando mujeres ejercitándose en un gimnasio, donde se apreciaba el rostro de las mismas y su cuerpo, “subiendo”

las mismas a la página pornográfica junto a textos y descripciones “degradantes”. En el marco del proceso judicial se realizó un allanamiento en **los domicilios** del acusado, obteniendo teléfonos, ordenadores y discos externos. Se encontró pornografía infantil, mujeres grabadas en la vía pública sin el consentimiento de las mismas. También se prueba que utilizó la red wifi de su vecina para no ser descubierto y además que intercambio el material que obtuvo por medio de la red con terceros. Finalmente es condenado a 26 años de prisión, por los siguientes delitos:

- El delito de odio, a **1 año de prisión**, inhabilitación de sufragio y multa de 6 meses con cuota diaria de 3 euros con responsabilidad personal subsidiaria;
- **Por cada uno de los 24 delitos** contra la integridad moral a **1 año de prisión** e inhabilitación para el sufragio pasivo durante la condena,
- Por difundir material pornográfico conf. Art. 189 (pornografía infantil) a **1 año y 6 meses de prisión** e inhabilitación para cargos públicos o ejercicio de la profesión u oficio con menores durante 6 años;
- Por el delito de defraudación de telecomunicaciones la pena de multa de 1 mes con cuota diaria de 3 euros.
- Prohibición de acercamiento en un radio inferior a 500 metros a las personas, lugares de trabajo y domicilios mencionados, por 2 años y la prohibición de cualquier tipo de contacto por dicho tiempo. (Jurisprudencia española - Juicio 169/18, 2018).

Artículo 197 bis.

1. El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo,

Será castigado con pena de prisión de seis meses a dos años.

2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.

Artículo 197 ter.

Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:

a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o

b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Artículo 197 quater.

Si los hechos descritos en este Capítulo se hubieran cometido en el seno de una organización o grupo criminal, se aplicarán respectivamente las penas superiores en grado.

COMENTARIO:

Este artículo que incorpora un agravante es específicamente orientado a la ciberdelincuencia. Considero prudente su incorporación por la necesidad de reducir la misma y por otro lado observo que en este ordenamiento en cuestión esto es una prioridad.

Contemplando que ha crecido notablemente la delincuencia informática mediante la utilización de la Dark Web, a la que me referí en los primeros capítulos, este artículo apunta a penar de forma más severa a los delincuentes que se valgan de esta herramienta.

Artículo 197 quinquies. Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los artículos 197, 197 bis y 197 ter, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

Artículo 201. 1. Para proceder por los delitos previstos en este capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, persona con discapacidad necesitada de especial protección o una persona desvalida, también podrá denunciar el Ministerio Fiscal.

2. No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, (funcionario público que cometa

la acción sin mediar causa legal por delito)ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.

Artículo 198. Por otro lado el artículo 198 sobre el accionar de funcionarios públicos incorpora en su inciso 3 que: el perdón del ofendido o de su representante legal, en su caso, extingue la acción penal sin perjuicio de lo dispuesto en el segundo párrafo del número 5º del apartado 1 del artículo 130.

COMENTARIO:

*Algo a destacar es que la legislación penal Española contempla dentro del articulado de estos delitos el tipo de acción, es decir que establece (según nuestra concepción) la instancia privada y delito de acción pública para el supuesto de que sea cometido por un funcionario público **sin que medie una causa legal**. Respecto a esto destaco que el proyecto de Código Penal tiene un artículo aparte, donde se contempla que si el autor de estos delitos es un funcionario público la pena aumentará. Considero bastante útil esta redacción que engloba para estas conductas un agravante como el mencionado.*

Artículo 248. 1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2. También se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que fabricaren, introdujeran, poseyeran o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.

c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

Artículo 264. 1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años.

2. Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurre alguna de las siguientes circunstancias:

1.^a Se hubiese cometido en el marco de una organización criminal.

2.^a Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos.

3.^a El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad.

4.^a Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones.

5.^a El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter.

Si los hechos hubieran resultado de extrema gravedad, podrá imponerse la pena superior en grado.

3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

Artículo 264 bis. 1. Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno:

a) realizando alguna de las conductas a que se refiere el artículo anterior;

b) introduciendo o transmitiendo datos; o

c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica.

Si los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado.

2. Se impondrá una pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado, cuando en los hechos a que se refiere el apartado anterior hubiera concurrido alguna de las circunstancias del apartado 2 del artículo anterior.

3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

Artículo 400. La fabricación, recepción, obtención o tenencia de útiles, materiales, instrumentos, sustancias, datos y programas informáticos, aparatos, elementos de seguridad, u otros medios específicamente destinados a la comisión de los delitos descritos en los Capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.

COMENTARIO:

Se observa a simple vista que la redacción del articulado Español es más abarcativa que el desarrollado por nuestro país. Así la norma tiene una redacción que permite ser omnicomprensiva y a su vez no se autolimita en una serie de acotados términos, siendo útil y fácil de emplear.

Considero relevante que la sola tenencia de programas informáticos, entre otros, esté penada cuando el fin es cometer alguno de los delitos contemplados. En algunas ocasiones esto será más complicado de probar pero si se piensa específicamente en un sujeto que tenga en su poder un elemento para descifrar claves, a modo de ejemplo, será más sencillo identificar el porqué de su tenencia.

Artículo 573. 1. Se considerará delito de terrorismo la comisión de cualquier delito grave contra la vida o la integridad física, la libertad, la integridad moral, la libertad e indemnidad sexuales, el patrimonio, los recursos naturales o el medio ambiente, la salud pública, de riesgo catastrófico, incendio, de falsedad documental, contra la Corona, de atentado y tenencia, tráfico y depósito de armas, municiones o explosivos, previstos en el presente Código, y el apoderamiento de aeronaves, buques u otros medios de transporte colectivo o de mercancías, cuando se llevaran a cabo con cualquiera de las siguientes finalidades:

1.^a Subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo.

2.^a **Alterar gravemente la paz pública.**

3.^a Desestabilizar gravemente el funcionamiento de una organización internacional.

4.^a **Provocar un estado de terror en la población o en una parte de ella.**

2. Se considerarán igualmente delitos de terrorismo los delitos informáticos tipificados en los artículos 197 bis y 197 ter (acceso a programas y datos) y 264 a 264 quater cuando los hechos se cometan con alguna de las finalidades a las que se refiere el apartado anterior.

3. Asimismo, tendrán la consideración de delitos de terrorismo el resto de los delitos tipificados en este Capítulo.

COMENTARIO:

Todo este articulado es el reflejo de una duda que inserté en el primer capítulo. Si la difusión de delitos por internet o la transmisión de mensajes que arenguen a las masas a cometer un ilícito, podría ser una nueva figura de apología del delito o bien debía ser considerado un tipo aparte. Es claro que el impacto social de estas conductas es alto y llega a alterar la paz pública como bien contempla la norma. Además genera un grado de terror tal que es considerado por el legislador a la hora de penar estas acciones. Para la legislación Española esto constituye un tipo a parte y está directamente relacionado con los delitos informáticos. Encuentro sumamente ponderable tal redacción por ser comprensiva de los fenómenos actuales y por estar a la altura de la realidad.

Me resulta admirable desde distintos puntos de vista y creo que es un precepto normativo que deberíamos adoptar.

3. United States - Estados Unidos

Como es de público conocimiento la legislación en estados unidos puede ser federal o bien puede variar en cada estado. Respecto a los delitos informáticos hay una crítica generalizada que trasciende cada vez con mayor frecuencia; hay una legislación que regula este fenómeno pero varía en cada estado, es decir que carecen de una normativa federal.

Se incorporarán distintos Códigos con el fin de mostrar la variada normativa que puede adoptarse dentro de un territorio con el fin de dar pelea a los delitos informáticos. La selección de legislaciones se realizará en base a distintos estados con mayor densidad poblacional.

3.1 U.S CODE - CÓDIGO DE LOS ESTADOS UNIDOS.

(a) Whoever, in the special maritime and territorial jurisdiction of the United States, has the intent to capture an image of a private area of an individual without their consent, and knowingly does so under circumstances in which the individual has a reasonable expectation of privacy, shall be fined under this title or imprisoned not more than one year, or both.

(b) In this section—

(1) the term “capture”, with respect to an image, means to videotape, photograph, film, record by any means, or broadcast;

(2) the term “broadcast” means to electronically transmit a visual image with the intent that it be viewed by a person or persons;

(3) the term “a private area of the individual” means the naked or undergarment clad genitals, pubic area, buttocks, or female breast of that individual;

(4) the term “female breast” means any portion of the female breast below the top of the areola; and

(5) the term “under circumstances in which that individual has a reasonable expectation of privacy” means—

(A) circumstances in which a reasonable person would believe that he or she could disrobe in privacy, without being concerned that an image of a private area of the individual was being captured; or

(B) circumstances in which a reasonable person would believe that a private area of the individual would not be visible to the public, regardless of whether that person is in a public or private place.

Dentro del título 18, Capítulo XVIII, el artículo 1801 indica que: quien, en la jurisdicción marítima y territorial de los Estados Unidos, tenga la intención de capturar una imagen de un área privada de un individuo sin su consentimiento, y lo haga a sabiendas de que el individuo tenga una expectativa razonable de privacidad, será multado bajo este título o encarcelado no más de un año, o ambos.

1 el término " captura ", con respecto a una imagen, significa grabar en video, fotografiar, filmar, grabar por cualquier medio o transmitir ;

2 el término " transmisión " significa transmitir electrónicamente una imagen visual con la intención de que sea vista por una persona o personas;

3 el término " un área privada del individuo " significa los genitales desnudos o vestidos con ropa interior, el área pública, las nalgas o el seno femenino de ese individuo;

4 el término " seno femenino " significa cualquier porción del seno femenino debajo de la parte superior de la areola; y

5 el término " en circunstancias en que ese individuo tiene una expectativa razonable de privacidad " significa que contempla circunstancias en las que una persona creería que podría desvestirse en la intimidad, sin preocuparse de que se capturara una imagen de un área privada ; o circunstancias en las que una persona razonable creería que un área privada del individuo no sería visible para el público, independientemente de si esa persona está en un lugar público o privado. (CÓDIGO PENAL DE ESTADOS UNIDOS).

3.2 **PENAL CODE- CÓDIGO PENAL DE CALIFORNIA.**

(a) Every person who, with intent to extort property or other consideration from another, sends or delivers to any person any letter or other writing, whether subscribed or not, expressing or implying, or adapted to imply, any threat such as is specified in Section 519 is punishable in the same manner as if such property or other consideration were actually obtained by means of such threat.

(b) (1) Every person who, with intent to extort property or other consideration from another, introduces ransomware into any computer, computer system, or computer network is punishable pursuant to Section 520 in the same manner as if such property or other consideration were actually obtained by means of the ransomware.

(2) Prosecution pursuant to this subdivision does not prohibit or limit prosecution under any other law.

(c) (1) "Ransomware" means a computer contaminant, as defined in Section 502, or lock placed or introduced without authorization into a computer, computer system, or computer network that restricts access by an authorized person to the computer, computer system, computer network, or any data therein under circumstances in which the person responsible for the placement or introduction of the ransomware

demands payment of money or other consideration to remove the computer contaminant, restore access to the computer, computer system, computer network, or data, or otherwise remediate the impact of the computer contaminant or lock.

(2) A person is responsible for placing or introducing ransomware into a computer, computer system, or computer network if the person directly places or introduces the ransomware or directs or induces another person to do so, with the intent of demanding payment or other consideration to remove the ransomware, restore access, or otherwise remediate the impact of the ransomware.

Este Código, en su primera parte, Título 13, Capítulo 7 sancionado en 1872; tuvo una reciente modificación en el año 2017, así se incorporó a la tipificación de delitos informáticos, el ransomware.

523 (a) Toda persona que, con la intención de extorsionar la propiedad u otra consideración de otra persona, envíe o entregue a cualquier persona cualquier carta u otro escrito, ya sea suscrito o no, expresando o implicando, o adaptado para implicar, cualquier amenaza como se especifica en la Sección 519 es punible de la misma manera que si tal propiedad u otra consideración se obtuviera realmente por medio de tal amenaza.

(b) (1) Toda persona que, con la intención de extorsionar propiedad u otra consideración de otro, introduzca ransomware en cualquier computadora, sistema informático o red informática, es punible de conformidad con la Sección 520 de la misma manera que si dicha propiedad u otra consideración en realidad se obtuvieron por medio del ransomware.

(2) El enjuiciamiento conforme a esta subdivisión no prohíbe ni limita el enjuiciamiento bajo ninguna otra ley. (c) (1) "Ransomware" significa un contaminante informático, como se define en la Sección 502, o un candado colocado o introducido sin autorización en una computadora, sistema informático o red informática que restringe el acceso de una persona autorizada a la computadora, sistema informático, red informática o cualquier dato en los mismos en circunstancias en que la persona responsable de la colocación o introducción del ransomware exige el pago de dinero u otra consideración para eliminar el contaminante informático, restaurar el acceso a la computadora, sistema informático, red informática o datos, o remediar el impacto del contaminante o bloqueo de la computadora.

(2) Una persona es responsable de colocar o introducir ransomware en una computadora, sistema informático o red informática si la persona coloca o introduce

directamente el ransomware o lo dirige o induce a otra persona a hacerlo, con la intención de exigir el pago u otra consideración para eliminar el ransomware, restaurar el acceso o remediar el impacto del ransomware. *(Modificado en 2017, Capítulo 518, Sec. 3. (SB 500) Efectivo el 1 de enero de 2018).* (PENAL CODE CALIFORNIA)

3.3.B NEW YORK PENAL LAW - Ley Penal de Nueva York.

Section 250.25 Tampering with private communications Penal (PEN)

A person is guilty of tampering with private communications when:

1. Knowing that he does not have the consent of the sender or receiver, he opens or reads a sealed letter or other sealed private communication; or 2. Knowing that a sealed letter or other sealed private communication has been opened or read in violation of subdivision one of this section, he divulges without the consent of the sender or receiver, the contents of such letter or communication, in whole or in part, or a resume of any portion of the contents thereof; or 3. Knowing that he does not have the consent of the sender or receiver, he obtains or attempts to obtain from an employee, officer or representative of a telephone or telegraph corporation, by connivance, deception, intimidation or in any other manner, information with respect to the contents or nature thereof of a telephonic or telegraphic communication; except that the provisions of this subdivision do not apply to a law enforcement officer who obtains information from a telephone or telegraph corporation pursuant to section 250.35; or 4. Knowing that he does not have the consent of the sender or receiver, and being an employee, officer or representative of a telephone or telegraph corporation, he knowingly divulges to another person the contents or nature thereof of a telephonic or telegraphic communication; except that the provisions of this subdivision do not apply to such person when he acts pursuant to section 250.35. Tampering with private communications is a class B misdemeanor.

(...) 1. "Sexual or other intimate parts" means the human male or female genitals, pubic area or buttocks, or the female breast below the top of the nipple, and shall include such part or parts which are covered only by an undergarment.

2. "Broadcast" means electronically transmitting a visual image with the intent that it be viewed by a person.

3. "Disseminate" means to give, provide, lend, deliver, mail, send, forward, transfer or transmit, electronically or otherwise to another person.

4. "Publish" means to (a) disseminate, as defined in subdivision five of this section, with the intent that such image or images be disseminated to ten or more persons; or (b) disseminate with the intent that such images be sold by another person; or (c) post, present, display, exhibit, circulate advertise or allows access, electronically or otherwise, so as to make an image or images available to the public; or (d) disseminate with the intent that an image or images be posted, presented, displayed, exhibited, circulated, advertised or made accessible, electronically or otherwise and to make such image or images available to the public.

Parte 3°, Título “N”, Artículo 250, determina cuando una persona es culpable de alterar las comunicaciones privadas:

1. Sabiendo que no tiene el consentimiento del remitente o receptor, abre o lee una carta sellada u otra comunicación privada sellada; o

2. Sabiendo que una carta sellada u otra comunicación privada sellada se ha abierto o leído en violación de la subdivisión de esta sección, divulga sin el consentimiento del remitente o receptor, el contenido de dicha carta o comunicación, en su totalidad o en parte, o un resumen de cualquier parte de su contenido; o

3. Sabiendo que no tiene el consentimiento del remitente o receptor, obtiene o intenta obtener de un empleado, funcionario o representante de una corporación telefónica o telegráfica, por connivencia, engaño, intimidación o de cualquier otra manera, información con respecto a los contenidos o naturaleza de los mismos de una comunicación telefónica o telegráfica; excepto que las disposiciones de esta subdivisión no se aplican a un agente de la ley que obtiene información de una corporación telefónica o telegráfica ; 4. Sabiendo que no tiene el consentimiento del remitente o receptor, y siendo un empleado, funcionario o representante de una corporación telefónica o telegráfica, a sabiendas divulga a otra persona el contenido o la naturaleza de una comunicación telefónica o telegráfica; excepto que las disposiciones de esta subdivisión no se aplican a dicha persona cuando actúa de conformidad con la sección 250.35 . La manipulación de las comunicaciones privadas es un delito menor de clase B.

- “Partes sexuales u otras partes íntimas ” significa los genitales humanos masculinos o femeninos, el área púbica o las nalgas, o el seno femenino debajo de la parte superior del pezón, e incluirá dicha parte o partes que están cubiertas solo por una prenda interior.

- **"Transmitir "** significa transmitir electrónicamente una imagen visual con la intención de que sea vista por una persona.

- **" Difundir "** significa dar, proporcionar, prestar, entregar, enviar, enviar, reenviar, transferir o transmitir, electrónicamente o de otra manera a otra persona.

- **" Publicar "** significa (a) difundir, como se define en la subdivisión cinco de esta sección, con la intención de que dicha imagen o imágenes se difundan a diez o más personas; o (b) difundir con la intención de que esas imágenes sean vendidas por otra persona; o (c) publicar, presentar, exhibir, exhibir, circular, publicitar o permitir el acceso, electrónicamente o de otro modo, para poner una imagen o imágenes a disposición del público; o (d) difundir con la intención de que una imagen o imágenes se publiquen, presenten, muestren, exhiban, circulen, anuncien o hagan accesibles, electrónicamente o de otro modo, y que dichas imágenes o imágenes estén disponibles para el público.

A person is guilty of unlawful surveillance in the second degree when:

1. For his or her own, or another person's amusement, entertainment, or profit, or for the purpose of degrading or abusing a person, he or she intentionally uses or installs, or permits the utilization or installation of an imaging device to surreptitiously view, broadcast or record a person dressing or undressing or the sexual or other intimate parts of such person at a place and time when such person has a reasonable expectation of privacy, without such person's knowledge or consent; or
2. For his or her own, or another person's sexual arousal or sexual gratification, he or she intentionally uses or installs, or permits the utilization or installation of an imaging device to surreptitiously view, broadcast or record a person dressing or undressing or the sexual or other intimate parts of such person at a place and time when such person has a reasonable expectation of privacy, without such person's knowledge or consent; or
3. (a) For no legitimate purpose, he or she intentionally uses or installs, or permits the utilization or installation of an imaging device to surreptitiously view, broadcast or record a person in a bedroom, changing room, fitting room, restroom, toilet, bathroom, washroom, shower or any room assigned to guests or patrons in a motel, hotel or inn, without such person's knowledge or consent. (b) For the purposes of this subdivision, when a person uses or installs, or permits the utilization or installation of an imaging device in a bedroom, changing room, fitting room, restroom, toilet, bathroom, washroom, shower or any room assigned to guests or patrons in a hotel, motel or inn, there is a rebuttable

presumption that such person did so for no legitimate purpose; or

4. Without the knowledge or consent of a person, he or she intentionally uses or installs, or permits the utilization or installation of an imaging device to surreptitiously view, broadcast or record, under the clothing being worn by such person, the sexual or other intimate parts of such person; or

5. For his or her own, or another individual's amusement, entertainment, profit, sexual arousal or gratification, or for the purpose of degrading or abusing a person, the actor intentionally uses or installs or permits the utilization or installation of an imaging device to surreptitiously view, broadcast, or record such person in an identifiable manner: (a) engaging in sexual conduct, as defined in subdivision ten of section 130.00 of this part; (b) in the same image with the sexual or intimate part of any other person; and (c) at a place and time when such person has a reasonable expectation of privacy, without such person's knowledge or consent.

Unlawful surveillance in the second degree is a class E felony.

Art. 250.45: Una persona es culpable de vigilancia ilegal en segundo grado cuando:

1. Para su propio entretenimiento o para el entretenimiento o el beneficio de otra persona, o con el propósito de degradar o abusar de una persona, él o ella usa o instala intencionalmente, o permite la utilización o instalación de un dispositivo de imágenes para ver subrepticamente, transmita o grabe a una persona vistiéndose o desvestiéndose o las partes sexuales u otras partes íntimas de dicha persona en un lugar y momento en que dicha persona tenga una expectativa razonable de privacidad, sin el conocimiento o consentimiento de dicha persona; o

2. Para su propia excitación sexual o la satisfacción sexual de otra persona, él o ella usa o instala intencionalmente, o permite la utilización o instalación de un dispositivo de imágenes para ver, transmitir o grabar subrepticamente a una persona vistiendo o desvestiéndose o u otras partes íntimas de dicha persona en un lugar y momento cuando dicha persona tiene una expectativa razonable de privacidad, sin el conocimiento o consentimiento de dicha persona; o

3. (a) Sin un propósito legítimo, él o ella usa o instala intencionalmente, o permite la utilización o instalación de un dispositivo de imágenes para ver, transmitir o grabar subrepticamente a una persona en un dormitorio, vestuario, probador, baño, ducha o cualquier habitación asignada a huéspedes o clientes en un motel, hotel u posada, sin el conocimiento o consentimiento de dicha persona.

(b) Para los propósitos de esta subdivisión, cuando una persona usa o instala, o permite la utilización o instalación de un dispositivo de imágenes en un dormitorio, vestuario, probador, baño, baño, baño, baño, ducha o cualquier habitación asignada Para los huéspedes o clientes en un hotel, motel o posada, existe una presunción refutable de que esa persona lo hizo sin ningún propósito legítimo; o

4. Sin el conocimiento o consentimiento de una persona, él o ella usa o instala intencionalmente, o permite la utilización o instalación de un dispositivo de imágenes para ver, transmitir o grabar subrepticamente, debajo de la ropa que usa esa persona, el sexual u otras partes íntimas de tal persona; o

5. Para la diversión, entretenimiento, lucro, excitación o satisfacción sexual propia o de otra persona, o con el propósito de degradar o abusar de una persona, el actor usa o instala o permite intencionalmente la utilización o instalación de un dispositivo de imagen para ver subrepticamente, transmitir o grabar a dicha persona de manera identificable:

(a) participar en conducta sexual, como se define en la subdivisión diez de la sección 130.00 de esta parte;

(b) en la misma imagen con la parte sexual o íntima de cualquier otra persona; y (c) en un lugar y momento en que dicha persona tiene una expectativa razonable de privacidad, sin el conocimiento o consentimiento de dicha persona.

La vigilancia ilegal en segundo grado es un delito mayor de clase E. (New York Penal Law).

COMENTARIO:

Si bien se contemplan situaciones tendientes a proteger la esfera de privacidad de los sujetos, la legislación penal estadounidense no otorga un foco orientado exclusivamente a los delitos informáticos sino que, muy por el contrario, lo hace extensivo a cualquier situación donde la privacidad de una persona pueda ser vulnerada. Por otro lado respecto a delitos informáticos pondero que se tipifique las conductas realizadas valiéndose de un ransomware, ya que es una forma actual de cometer “ciberataques”.

Pudiendo agregar más contenido de esta índole, doy por finalizado la incorporación de legislación Estadounidense y extranjera, habiendo expuesto la diversidad legislativa en la actualidad.

Capítulo 5- “Consideraciones finales”.

El autor mexicano Julio T. Valdez contemplaba por allá en el 2008 que el atraso en la legislación de estas conductas generaba efectos negativos. Actualmente México modificó su legislación, sin embargo las reflexiones del autor encuadran perfectamente en la situación de la Argentina.

Así opinaba que: “En el caso de considerar este tipo de ilícitos como figuras análogas existentes se corre el riesgo de alterar de manera flagrante el principio de legalidad de las penas. Cabe mencionar que una adecuada legislación al respecto traería consigo efectos no sólo correctivos sino eventualmente preventivos, de tal forma que se reducirían en gran número este tipo de acciones que tanto daño causan a los intereses individuales y sociales. El objetivo de crear un espacio de libertad, seguridad y justicia debe ser alcanzado mediante la prevención y la lucha contra la delincuencia, organizada o no, incluido el terrorismo, mediante una cooperación más estrecha entre los servicios represivos y las autoridades judiciales de los distintos Estados interesados, armonizando las legislaciones y las normativas en materia de cooperación policial y judicial penal.” (Tellez Valdez, 2008, p. 207)

En conclusión la legislación actual deja situaciones fuera de la órbita de comprensión jurídica, facilitando que Argentina sea un lugar atractivo para cometer delitos informáticos no contemplados en la ley penal.

Por otro lado los cuatro pilares fundamentales son los encargados de brindar una aparente solución a tal problemática. No puede negarse que hoy en día todo pasa por Internet y los sujetos que utilizan distintas redes sociales ven como muchos de sus derechos reconocidos en el mundo físico se vuelven letra muerta cuando se trata de la Web. Con motivo de brindar una protección adecuada a los derechos personalísimos, el derecho debe estar al servicio de la comunidad, haciéndose presente por medio de legislación capaz de afrontar las nuevas problemáticas.

Es claro que muchas víctimas no pueden ejercer su derecho a denunciar ciertos hechos padecidos en la web por inexistencia de tipos y eso hoy constituye una de las barreras más grandes, lo que impide que se pueda acceder a la justicia.

Debe seguirse los pasos de otros ordenamientos jurídicos, donde hay puntos comunes en la legislación penal.

Respecto a la Argentina se puede observar con claridad que el foco de protección está en el ámbito patrimonial, es decir que en su mayoría y con excepción de la pornografía infantil, se busca proteger el patrimonio de las víctimas lejos de cuidar la esfera extrapatrimonial. Así se contempla que figuras como la violación de secretos y las injurias parecen tener su precepto normativo actualizado, pero lejos de ser así obvian nuevas situaciones que pueden realizarse por internet.

Sobre la legislación de estas conductas se debe remarcar el aspecto positivo de legislarlas: en el contexto actual puede ser tildado de “censura previa” o de coartar la libertad de expresión en Internet; lo cierto es que estas son opiniones infundadas y realizadas con un corto análisis del panorama. Lo que trae aparejado contemplar estas situaciones en la norma penal es la delimitación de las conductas que serán penadas, la protección a determinados bienes jurídicos y el esclarecimiento de en qué circunstancias y bajo qué aspectos se puede investigar determinado hecho. Muy por el contrario de lo que puede especularse esto traerá claros beneficios para la sociedad, desde una norma que proteja a los usuarios de internet, el acceso a la justicia por parte de las víctimas, la inclusión de normas sobre cooperación internacional, etc. Una vez que se encuentren legisladas el índice de denuncias aumentará pero será efecto de que exista el tipo a denunciar, lo cual es positivo para contabilizar la totalidad de los casos.

Por otro lado para resolver rápidamente las denuncias se deben realizar procesos breves que permitan la defensa del imputado pero permita un actuar rápido de la justicia. Con el paso del tiempo y el funcionamiento de los cuatro pilares fundamentales siendo: Una normativa penal, políticas activas por parte del Estado, la tecnología como una herramienta de prevención y la Cooperación Internacional; el índice de comisión de estas conductas disminuirá.

En el contexto actual se genera una doble vulneración de los derechos, cuando se comete la conducta disvaliosa y cuando no hay una norma que los prevenga y sancione. ¿De qué serviría que haya un derecho reconocido si no hay una norma que proteja la violación de los mismos? Esta es la situación actual de los delitos informáticos extrapatrimoniales. El derecho a la privacidad, intimidad, libertad y honor, están reconocidos Constitucionalmente, pero el derecho penal no da una respuesta, aún.

Hubo poco esfuerzo normativo, el que genera una doble vulneración.

Lo cierto es que la garantía Constitucional es otro de los fundamentos para la existencia de este tipo de normas.

Si bien es cierto que debe tratarse con cuidado la imposición de penas privativas de la libertad, es algo que no puede ser apartado del análisis. Esto se debe a que la situación del país es un tanto delicada ya que las condiciones carcelarias son pésimas, inhumanas y la discusión del fin de la pena vuelve a estar en boga. Por otro lado es evidente que debe resolverse esto con brevedad pero no por esto se negara la imposición de este tipo de penas para estos delitos. Y es en base a esto que en el capítulo primero donde desarrolle “las nuevas conductas susceptibles de ser tipificadas” no asigne ninguna escala penal como “sugerida” para ser impuesta. Porque creo que debe estudiarse contemplando otras legislaciones y es allí donde entra en juego el derecho comparado. Lo que creo razonable es la existencia de un equilibrio, pero si tomamos como ejemplo la Jurisprudencia Española indicada en el Capítulo 4º, donde se condena por 26 años de prisión a un sujeto por las conductas descriptas, parecería un tanto elevado; comparando claro las escalas penales asignadas por nuestra justicia, normalmente. Es por esto que deberá estudiarse a fondo por parte del legislador cual será la solución más adecuada. Si imponer una pena privativa de la libertad que contemple una escala mínima o bien incorporar multas muy elevadas; destacando por supuesto que este último supuesto no lo comparto ya que la norma penal debe generar respeto en el individuo; de lo contrario será letra muerta. A raíz del interrogante sobre la escala penal más adecuada, que surge como consecuencia de sugerir nuevos tipos debo incluir la solución que creo más acertada y que compartiré en el siguiente y ultimo subtítulo denominado “propuestas”.

Es muy cierto, por otro lado, que la sola existencia de una norma bien redactada y capaz de comprender la mayoría de los supuestos, no detendrá la comisión de los delitos en general. No obstante esto podría ser observado de manera distinta en lo que respecta a los delitos informáticos extrapatrimoniales, ya que no son motivados por una necesidad económica que afecte al autor sino que son, por el contrario, cometidos con el fin de dañar distintos aspectos de la vida de otro ser humano, entonces al existir una legislación que penalice estas conductas habrá un porcentaje de disminución de comisión; por generar cierto temor. La seguridad que tiene el sujeto de que no será “atrapado” y de que puede valerse de distintas herramientas informáticas para cubrir su identidad motivará a que estos delitos crezcan; en cambio las políticas activas por parte del Estado generarán una merma de estas situaciones, ¿Cómo? Haciendo público que

hay fiscalías especializadas en estos delitos, que ya hay una norma que comprenda estas situaciones, que se publiquen las estadísticas de denuncias y casos donde se identificó al autor y se lo puso a disposición de la justicia; generando conciencia de que el Estado tomó parte en la problemática y será de gran ayuda para evitar la proliferación de estas conductas.

Así los delitos extrapatrimoniales son manejables desde los cuatro pilares fundamentales.

Por último no puede dejarse fuera de la conclusión que la reforma del Código Penal es sin duda necesaria.

Resultará evidente al analizar este trabajo que no podrán brindarse cifras oficiales sobre el índice de estos hechos, en primer lugar por no tener un lugar en la legislación penal y en segundo lugar por la falta de organización que suele padecer nuestro país cuando se trata de estadísticas que evidencien nuestros problemas. Creo sin lugar a dudas que se deben tomar medidas de transparencia para resolver de una vez por todos los problemas que nos atañen.

Propuestas:

1. Se tipifiquen las siguientes conductas:

a. *Imponer prisión al que suplante la identidad de un tercero en una red social o cualquier plataforma digital, introduciendo cualquier tipo de contenido sobre uno o más sujetos, sea revelando secretos, o bien introduciendo datos falsos para generar cualquier tipo de perjuicio.*

Imponer prisión para el o los que difundan cualquier representación visual, auditiva o audiovisual, de una o más personas realizando actos sexuales o de

b. *contenido íntimo por medio de canales electrónicos, cualquier red social o plataforma digital. Siendo que el contenido pudo haberse generado a conciencia del perjudicado o sin que este supiera; pero **sin que hubiere autorizado dicha difusión.***

c. *Crear, modificar para potenciar su peligrosidad, enseñar a utilizar, distribuir, publicar, un malware con el fin de vulnerar la seguridad de usuarios en internet y así causar un perjuicio patrimonial y/o extrapatrimonial.*

d. *Espiar comunicaciones, representaciones de una o más personas; en cuanto a su imagen y/o voz, por medio de cualquier herramienta que pueda ser empleada vulnerando sistemas de seguridad o aprovechándose de su falta de seguridad, generando un perjuicio a la intimidad y el secreto de una o más personas.*

e. *Crear representaciones visuales y/o audiovisuales de una o más personas para publicarlas sin su consentimiento, con fines que no coincidan con el bien común o el orden público.*

f. *Publicar la comisión de delitos por redes sociales, plataformas de contenido digital, o internet; para incitar a que una o más personas comenten ese delito.*

2. Que estos tipos sean de acción pública. Es claro que al ser delitos que afectan una fibra muy sensible de la víctima en pocas ocasiones se realiza la denuncia. Estableciendo entonces que sean de acción pública la justicia en tanto tome conocimiento de un hecho de estas características podrá actuar de oficio.

3. Que la escala penal contemplada para los delitos de agresión extrapatrimonial; incisos: a, b, c (si ocasiona un perjuicio extrapatrimonial), d,e, sea de: UN (1) año de prisión a CUATRO (4) años. Y de SEIS (6) meses a TRES (3) años para aquel delito aquí numerado, que solamente dañe la esfera patrimonial.

La razón de ser de la escala penal se basa en un equilibrio entre las escalas penales contempladas para todos los delitos en contra de la integridad sexual y las penas propuestas en el anteproyecto de Código Penal del pasado 2019.

Así la pena de prisión o reclusión más baja es la que sugiero debe aplicarse para estas conductas.

A saber: Según el artículo 500 de dicho proyecto de ley, la pena máxima contemplada para los delitos informáticos contemplados en el Título XXVI, es de SEIS (6) años, esa pena es para aquel que defraude a otro alterando o suprimiendo datos de un sistema informático o bien altere una transmisión de datos.

Por otro lado la pena mínima consiste en DOCE (12) días- multa por un mero daño informático.

4. Que, conforme los cuatro pilares mencionados se impulse la celebración de tratados internacionales que faciliten la investigación para estos hechos.

5. Crear más fiscalías especializadas en estos delitos, en función de la densidad poblacional dentro del territorio argentino.

Para terminar, ya habiendo delimitado las conductas disvaliosas, brindado la solución pertinente, recalcado la necesidad de incorporar normativa de palabras “amplias” en relación a la tecnología y habiendo argumentado la necesidad de regular estos tipos (conf. Capítulo 3 y otros); me resulta primordial recordar que los derechos que están en “juego” ante esta situación normativa, son elementales para la vida de cualquier ser humano. El derecho debe encargarse de proteger con límites claros toda invasión a las esferas más íntimas de los sujetos. Al fin y al cabo este derecho reconocido constitucionalmente no puede ser objeto de reiteradas violaciones por parte de terceros y mucho menos ser objeto de negocio.

El derecho debe evitar la muerte de la privacidad.

ÍNDICE

<i>Breve resumen de la problemática.</i>	1
<i>Objetivos:</i>	2
<i>Hipótesis:</i>	3
<i>Justificación en la elección del tema:</i>	4
<i>Problema jurídico relevante:</i>	6
<i>Introducción.</i>	7
Capítulo 1- “El derecho penal y sus espacios olvidados.”	15
1.Apertura del capítulo 1°	15
2.Principios en materia penal	18
3.¿Nuevas formas de cometer delitos?.....	23
3. 1 Las “novedosas” conductas susceptibles de ser tipificadas.....	24
3.2 Análisis de la estructura del delito adecuada a la problemática	33
4.Pilares fundamentales que aspiran a la solución de la problemática.	36
4.1 La normativa penal:	37
4.2 La tecnología como una herramienta de prevención.	40
4.3 Políticas activas por parte del Estado.....	41
4. 5 Una forma de Cooperación Internacional.....	42
Capítulo 2- “Normativa penal en la actualidad”.	45
Ley N° 26.388 - ¿Desenlace del problema?	46
Enmendando una omisión, Ley N° 27.436.	48
Sobre la responsabilidad de los proveedores:.....	51
Jurisprudencia vinculada.	53
Rodríguez María Belén c/ Google.	54
Ley de datos personales, N° 25.326.....	56
El escenario normativo luego de la ley N° 26.388:.....	58
El Anteproyecto del Código Penal de 2019	59
Desde una óptica Internacional:	67
EL CONVENIO DE BUDAPEST.....	67
Medidas que deben adoptarse:.....	68
Resolución 234/2016	72
Resolución 1291/19	74
Resolución 977/19	74
Cierre de capítulo.....	75
Capítulo 3 – “La vulneración de derechos constitucionales en la red”.	76

Análisis del derecho a la intimidad.....	78
Consideraciones jurisprudenciales sobre este derecho	81
Ciclo de conferencias maestros del Derecho, vinculado con el trabajo final:.....	82
Protección otorgada por Tratados internacionales.....	84
1.DECLARACIÓN AMERICANA DE LOS DEBERES Y DERECHOS DEL HOMBRE.....	84
2.DECLARACIÓN UNIVERSAL DE LOS DERECHOS HUMANOS.	86
3.CONVENCIÓN AMERICANA SOBRE DERECHOS HUMANOS- PACTO DE SAN JOSÉ DE COSTA RICA	86
La protección a la imagen	87
Protección al honor y reputación, sus alcances.	88
La identidad digital	89
Capítulo 4- “Una mirada al Derecho comparado”.	90
1.Brasil	90
a.Marco civil de internet	90
b.CÓDIGO PENAL DE BRASIL.	93
2.España	96
a.CÓDIGO PENAL DE ESPAÑA.	96
COMENTARIO y JURISPRUDENCIA:	97
COMENTARIO SOBRE LA JURISPRUDENCIA:	99
3.United States - Estados Unidos	105
3.1 U.S CODE - CÓDIGO DE LOS ESTADOS UNIDOS.	106
Capítulo 5- “Consideraciones finales”.	114
ÍNDICE	120
Bibliografía.....	122
Reserva de tema.....	126
Solicitud de tutoría.....	127

Bibliografía

General:

1. Código Penal de la Republica Argentina. (1985). *Ley N° 11.179*.
2. Constitución de la Nación, Ley N° 24.430. (s.f.).
3. Comprender el derecho, Conferencias de la Universidad Abierta Interamericana. (Diciembre de 2014). Buenos Aires.
4. Asamblea general ONU. (10 de Diciembre de 1948). Declaración universal de los derechos humanos.
5. Convenio sobre cibercriminación del consejo de Europa. (2017). Adhesión al Convenio de Budapest Ley N° 27.411. Buenos Aires.
6. Creus, C. (2010). *Derecho penal parte general* (Quinta ed.). Buenos Aires: Astrea de Alfredo y Ricardo Depalma.
7. Declaración americana de los deberes y derechos . (30 de Abril de 1948). Declaración. Colombia, Bogotá.
8. Declaración universal de los derechos humanos. (1948)
9. Ley 23.054. (1984). Aprobación Pacto san José de Costa Rica. Buenos Aires.
10. Principios de Manila. (2015). *Iniciativa de sociedad civil sobre la responsabilidad de los intermediarios, guías de buenas prácticas*.
11. LEY N° 12.965. (s.f.). Marco Civil Brasileño de Internet en Español. Brasil: Ediciones Camara
12. CÓDIGO PENAL DE BRASIL. (1940). Código penal brasileiro. Ley n° 2.848. (G. Translate, Trad.)
13. CÓDIGO PENAL DE ESPAÑA. (s.f.). Código penal español, Ley orgánica 10/1995. (Tít. VI, Capítulo III hta. Tít. XXI, Capítulo III). España.
14. Ley estadounidense- S. T. (s.f.). Internet Security and Privacy Act- Senado EEUU. – (Propia, Trad.).
15. New York Penal Law. (s.f.). Ley penal de Nueva York parte 3. (Propia, Trad.)
16. PENAL CODE CALIFORNIA. (s.f.). *PEN CALIFORNIA*. Obtenido de http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=PEN&division=&title=13.&part=1.&chapter=7.&article=
17. CÓDIGO PENAL DE ESTADOS UNIDOS. (s.f.). CÓDIGO PENAL EE.UU - Título 18, Capítulo 88. (Propia, Trad.) Estados Unidos.
18. Zaffaroni, E. R. (2005). *Manual de derecho penal: Parte general* (2da ed.). Buenos Aires: Ediar.
19. Tarrío Suárez, G., & Tarrío, M. C. (2015). *Manual de Derecho Penal parte general* (1ra ed.). Buenos Aires: Cathedra Jurídica.

20. Nuñez, R. C. (2009). *Manual de derecho penal*. Buenos Aires: Lerner.
21. ONU. (s.f.). Recuperado el 2019, de <https://www.un.org/ruleoflaw/es/thematic-areas/access-to-justice-and-rule-of-law-institutions/access-to-justice/>
22. ONU. (Abril de 2017). Recuperado el 2019, de https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2017/UNODC-CCPCJ-EG-4-2017-2/V1701129_S.pdf
23. Anteproyecto Código penal 2014. (2014). infojus. Obtenido de <https://www.telam.com.ar/advf/documentos/2014/04/53598b9463e9b.pdf>
24. 24/7, R. M.-R. (2019). Resolución 1291/19. Argentina.
25. 52/19, P. d.-E. (2019). Proyecto del Código penal. Buenos Aires, Argentina.
26. 977/19, R. (2019). Argentina.

Especial:

27. Alonso de Escamilla, A. (2019). *Ciberdelitos: El delito de Stalking como nueva forma de acoso* (2da ed.). Buenos Aires: Hammurabi.
28. Altmark, D. R., & Molina Quiroga, E. (2012). *Tratado de Derecho informático* (Primera ed., Vol. III). Buenos Aires: La ley.
29. Brandeis, L. D., & Warren, S. D. (1890). The right to privacy. *Harvard Law Review*, 4(5).
30. Bura Peralta, J. E. (2019). Acreditación y valoración judicial sobre calumnias e injurias a través de redes sociales. *El dial*.
31. Chervavsky, N. (2018). Centro de ciberseguridad Boletín 35. Buenos Aires.
32. de Cucco Alconada, M. C. (2018). *Saij.gob*. Recuperado el 2019
33. Donna, E. A. (2008). *Derecho penal parte general - Teoría general del delito I*. Rubinza Culzoni.
34. Fernández Delpech, H. (2016). *Manual de Derecho informático* (Primera ed.). Buenos Aires: AbeledoPerrot.
35. Guardiola Salmerón, M. (2016). Una sentencia sobre Stalking. España. *Revista de pensamiento penal*.
36. Hernandez Diaz, L. (2009). Recuperado el 2019, de <https://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf>
37. Martínez, A. N., & Porcelli, A. M. (s.f.). Alcances de la responsabilidad civil de los proveedores de servicios de internet y online a nivel internacional, regional y nacional.
38. Martinez, M. S. (2018).
39. Molina Quiroga, E. (2013). *Responsabilidad derivada de informes crediticios* (1ra ed.). Buenos Aires: La ley.

40. Nager, H. S. (2011). *Protección penal en la sociedad de la información- Análisis dogmático de los delitos informáticos Ley 26.388*. Buenos Aires: El dial .
41. Palazzi, P. A. (2016). *Los delitos informáticos en el Código penal, análisis de la ley 26388*. Buenos Aires: AbeledoPerrot.
42. Palazzi, P. A. (2019). *Delitos contra la intimidad informática*. Buenos Aires: CDYT.
43. Resio, M. (2018). *Delitos sexuales en la era digital*. Erreius.
44. Riande Juárez, N. A. (1998). Recuperado el 2019, de <http://www.ordenjuridico.gob.mx/Congreso/pdf/103.pdf>
45. Riquert, M. A. (2018). *Delitos informáticos en el anteproyecto del Código Penal de 2018*. Buenos Aires.
46. Riquert, M. A. (2019). *Ciberdelitos*. Buenos Aires: Hammurabi.
47. Rodriguez c/ Google inc. s/ Daños y perj., Rodriguez Maria Belen c/ Google Inc. s/ Daños y perj. (Corte Suprema de Justicia de la Nación 28 de Agosto de 2014).
48. Saguéz, N. P. (2003). *Elementos del derecho constitucional* (Vol. II). Buenos Aires: Astrea.
49. Sain, G. (2013). *El derecho penal aplicado a los delitos informáticos. ¿Una política eficiente para el cibercrimen?* Buenos Aires, Argentina: Infojus. Recuperado el 2019, de <http://www.pensamientopenal.com.ar/system/files/2014/04/doctrina38470.pdf>
50. Sain, G. (2018). *Revista de Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet*. Buenos Aires: Erreius.
51. Salt, M. (2017). *Diario Judicial*. Recuperado el 2019, de <https://www.diariojudicial.com/nota/77492/reportajes/necesitamos-legislar-sobre-medidas-para-la-obtencion-de-evidencia-digital.html>
52. Seguridad, P. g.-M. (2016). Resolución 234/16. Argentina.
53. Sueiro, C. C. (2011). *La eficiencia de la ley 26388 de reforma en materia de criminalidad informática al CPN. Ventajas y desventajas politico criminales*. Buenos Aires: El dial.
54. Tellez Valdez, J. (2008). *Derecho informático*. Mexico, México: Mc Graw Hill.
55. Temperini, M. G. (2018). Recuperado el 2019, de <http://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf>
56. Temperini, M. G. (s.f.). *Delitos informaticos en Latinoamerica, un estudio de Derecho comparado*. Recuperado el 2019, de <http://conaiisi.unsl.edu.ar/ingles/2013/82-553-1-DR.pdf>
57. Real Academia Española. (s.f.). *Diccionario de la lengua española*. Recuperado el 2019, de <https://dle.rae.es>
58. Informe de ciberseguridad- Observatorio . (2016). Recuperado el 2019, de <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion->

conocimiento/sites/agencia-gobierno-electronico-sociedad-informacion-
conocimiento/files/documentos/noticias/ciberseguridad-estamos-preparados-en-
america-latina-y-el-caribe.pdf

59. BBC. (2015). Recuperado el 2019, de
https://www.bbc.com/mundo/noticias/2015/08/150803_tecnologia_eeuu_pueblo_pago_rescate_malware_computadoras_lv.shtml
60. BBC. (2019). Recuperado el 2019, de
https://www.bbc.com/mundo/noticias/2015/08/150803_tecnologia_eeuu_pueblo_pago_rescate_malware_computadoras_lv.shtml
61. "El observador". (2019). Obtenido de <https://www.elobservador.com.uy/nota/amazon-se-une-a-facebook-y-microsoft-en-la-lucha-contr-a-el-deepfake-20191024134955>
62. ABC- España. (2019). Recuperado el 2019, de
https://www.abc.es/tecnologia/redes/abci-baltimore-ciudad-lleva-hackeada-peligroso-ransomware-robbinhood-201906070334_noticia.html
63. Info technology. (2017). Recuperado el 2019, de
<https://www.infotechnology.com/labs/Que-es-el-ransomware-el-secuestro-virtual-que-le-hace-perder-millones-a-las-empresas-20170512-0009.html>
64. **Diligencias urgentes- Jurisprudencia española**, 260/2016 (Juzgado de instrucción N° 3 2016).
65. **Jurisprudencia española** - Juicio 169/18, 201/2018 (Juzgado de lo penal N°2 2018).
66. **Corte Suprema de Justicia de la Nación**, Rodriguez, Maria Belén c/ Google Inc. s/ daños y perjuicios", 28/10/14.

Reserva de tema.

RE: Reserva de tema. Derecho. Sede centro



Marilina.Miceli@uai.edu.ar <Marilina.Miceli@uai.edu.ar>

30/8/2019 11:09

Para: m.aguyarov@gmail.com

Tema reservado. >Atte

Dra. Marilina Andrea Miceli
Secretaria Técnica de la
Facultad de Derecho y Cs. Políticas y
Directora de la carrera de Martillero publico,
Corredor y Administrador de consorcios
Universidad Abierta Interamericana
Tel. 4342-7788 int.139 Fax 4342-7654

De: Macarena Valenzuela [mailto:m.aguyarov@gmail.com]

Enviado el: jueves, 29 de agosto de 2019 04:06 p.m.

Para: Miceli, Marilina <Marilina.Miceli@UAI.edu.ar>

Asunto: Fwd: Reserva de tema. Derecho. Sede centro

De mi mayor consideración, Profesora Dra. Marilina Miceli.

Por el presente e-mail solicito hacer reserva de tema para mi trabajo final, con el objeto de obtener mi título de abogada. El tema del mismo versará sobre Los delitos informáticos en el anteproyecto del Código Penal.

Metodología:

Para la confección de mi trabajo consultaré investigaciones por parte de la doctrina y evaluaré el amterial audiovisual de juristas, como conferencia sobre Comprender el derecho, las cuales son llevadas a cabo por la Universidad Abierta Interamericana; además haré un análisis de jurisprudencia de la situación actual. Eventualmente compararé legislación internacional. Para llevar a cabo este trabajo le solicite asistencia al Profesor Dr. Gabriel González Da Silva, el cual será mi tutor; al cual le presente el proyecto de mi trabajo y está prestando su auxilio para que llegue a buen puerto.

Sin más que informar, saluda cordialmente,

Aguyaro Valenzuela Macarena. - Sede Centro

Solicitud de tutoría:

Buenos Aires, 19 de Julio de 2019.

De mi mayor consideración, Profesor Dr. Gabriel González Da Silva:

Por este medio es de mi agrado solicitarle que me preste asistencia para la elaboración de mi trabajo final, como mi tutor, con el objetivo de obtener el título de abogada.

El trabajo versará sobre los delitos informáticos en el anteproyecto del Código Penal. El tema que elegí llamo mi interés a partir de una serie de conferencias que visualice por Internet donde se discutía la situación de Argentina respecto la comisión de estos delitos. Al comenzar a investigar la situación en el resto del mundo observé el atraso legislativo que padecemos y provocó en mí elegirlo como tema de mi trabajo final.

Lo saluda cordialmente,

Aguyaro Valenzuela Macarena, alumna de sede Centro.